内 容 简 介

本书是作者在几所大学授课时所使用讲义的基础上，经多次修改和补充而成。全书共分五章：第一章域的扩张，第二章代数扩张，第三章 Galois理论，第四章超越扩张，第五章整扩张。作者在题材的选择和安排上，着眼于域的基本理论和基本方法以及对于其他学科应用较多的内容，给只具有高等代数及抽象代数初步知识的读者提供了一本系统地学习域论基础的书。

本书可做大学数学系学生的教材或教参。

ЛT.5/23

序

域是代数学中最基本的概念之一，历史悠久。早在十九世纪初叶，在 Galois 研究方程的著作中就有了域的概念的萌芽，虽然那时还没有域的抽象定义。1910年，Ernst Steinitz的论文《体的代数理论》，(Algebraische Theorie der Kōrper, J.reine und angew. Math. 137 (1910))问世。在这篇论文里，第一次对于域的理论作了全面、系统的阐述，奠定了域论的基础。时至今日，域论不仅本身是代数学中一个内容丰富的重要分支，而且也是学习其它一些分支，如代数数论，代数几何，环论，代数群等所不可缺少的基础知识，此外，有限域在近代的编码和计算机理论中都有着应用。

这本书最初是作者于1982年春应云南大学数学系之邀，在该系讲授域论时所编写的讲义，以后又经过多次修改和补充。共包括五章。第一章介绍域扩张及有关的一些最基本的概念，这是研究域的基本思想；第二章介绍代数扩张，其中对于可分性的问题作了较细致的讨论；第三章介绍 Galois 理论；第四章介绍超越扩张，包括超越基及超越次数，可分性，导子等；第五章介绍整扩张，包括环的整扩张，局部化及Hilbert零点定理等，这是交换代数的最基本的内容，有着广泛的应用。作者的意图是向只具有高等代数及抽象代数初步知识的读者提供一本系统地介绍域论基础的书。在题材的选择和安排上，着眼于域的基本理论和基本方法以及对于其它学科应用较多的内容，并不追求全面和完备，因此，对于有些本来应该属于域论的题材，如有序域，赋值等，就没有包括进去。

首先要感谢云南大学数学系的一些同事，正是由于他们的盛情邀请，才使作者想到要编写一本有关域方面的书。在编写过程中，我的许多同事曾给予不少帮助。特别是蒋滋梅同志，她不仅仔细地阅读了原稿，而且还用原稿作为讲义，在本校及外校讲授了数次，提出了很多宝贵的意见。谨在这里表示感谢。

希望读者批评指正。

郝钢新

1985年12月于

北京师范大学数学系

目　录

第一章 域的扩张

1.1 子域和扩域 添加

读者都已熟悉域的定义。一个域是一个至少有两个元素的集 F，在其中定义了两个代数运算，分别叫做加法和乘法；F 对于加法来说作成一个 Abel 群，F 的全体非零元素对于乘法来说作成一个 Abel 群，并且加法与乘法被分配律联系着。

设 F 是域 K 的一个子集。如果对于 K 的加法和乘法来说，F 本身也作成一个域，就称 F 是 K 的一个**子域**，而 K 是 F 的一个**扩域**，以后我们常常用符号 K/F 表示 K 是 F 的扩域，并且称为一个**域扩张**。

设 K/F 是一个域扩张。如果 E 是 K 的一个子域，同时又是 F 的一个扩域，就称 E 是域扩张 K/F 的一个**中间域**。

设 F 是域 K 的一个子域。T 是 K 的一个子集。令 $\{E_\alpha\}_{\alpha\in I}$（$I$ 是一个指标集）是域扩张 K/F 中包含 T 的中间域的全体。显然，$K\in\{E_\alpha\}_{\alpha\in I}$，所以 $\{E_\alpha\}_{\alpha\in I}\neq\varnothing$。令 $E=\bigcap\limits_{\alpha\in I}E_\alpha$。那么 E 是 K/F 的一个中间域。它是 K 中包含 F 和 T 的最小子域，记作 $F(T)$。称为添加 T 于 F 所得的扩域，或称为 T 在 F 上所生成的域。

当 $T=\{t_1,\cdots,t_n\}$ 是 K 的一个有限子集时，我们把 $F(T)$ 记作 $F(t_1,\cdots,t_n)$。这时就说 $F(t_1,\cdots,t_n)$ 是在 F 上**有限生成的**。特别，添加单独一个元素 t 于 F 所得的扩域 $F(t)$ 叫做 F 的一个**单扩域**。

定理 1.1.1 设 F 是域 K 的一个子域，T，T_1，T_2 都是 K

的子集。

（i） $F(T_1\cup T_2)=F(T_1)(T_2)$

（ii） 令$\{S_\alpha\}_{\alpha\in I}$是$T$的一切有限子集所成的子集族。那么

$$F(T)=\bigcup_{\alpha\in I}F(S_\alpha)$$

（iii） 设$T=\{t_1,\cdots,t_n\}$是有限集。那么

$$F(T)=\left\{\frac{f(t_1,\cdots,t_n)}{g(t_1,\cdots,t_n)}\,\middle|\, f,g\in F[X_1,\cdots,X_n],\ g(t_1,\cdots,t_n)\neq 0\right\}.$$

这里$F[X_1,\cdots,X_n]$是F上不相关不定元$X_1,\cdots,X_n$的多项式环。

证 (i) $F\subseteq F(T_1)(T_2)$，$T_1\cup T_2\subseteq F(T_1)(T_2)$，而$F(T_1\cup T_2)$是$K$的既包含$F$又包含$T_1\cup T_2$的最小子域，所以

$$F(T_1\cup T_2)\subseteq F(T_1)(T_2)。$$

反过来，$F(T_1)$是$F(T_1\cup T_2)$的子域，又$T_2\subseteq F(T_1\cup T_2)$。因为$F(T_1)(T_2)$是$K$的既包含$F(T_1)$又包含$T_2$的最小子域，所以

$$F(T_1)(T_2)\subseteq F(T_1\cup T_2)。$$

(ii) 由定义，对于每一个$\alpha\in I$，$F(S_\alpha)\subseteq F(T)$，从而$\bigcup_{\alpha\in I}F(S_\alpha)\subseteq F(T)$。

令$L=\bigcup_{\alpha\in I}F(S_\alpha)$。$L$是$K$的一个子域。事实上，设$u,v\in L$，那么存在$T$的有限子集$S_1$和$S_2$，使得$u\in F(S_1)$，$v\in F(S_2)$。令$S=S_1\cup S_2$，则$S$也是$T$的有限子集，并且$u,v\in F(S)$。由于$F(S)$是子域，所以$u+v$，$u-v$，$uv$，$uv^{-1}$（若$v\neq 0$）都属于$F(S)\subseteq L$。这就证明了$L$是$K$的子域。

现在设$t\in T$，那么$t\in F(t)\subseteq L$。因此$T\subseteq L$又$F\subseteq L$。所以$F(T)\subseteq L$。这样，

$$L=\bigcup_{\alpha\in I}F(S_\alpha)=F(T).$$

(iii) F的元素与 $t_1,\cdots,t_n$ 经过加、减、乘、除运算的结果都可以表示成以下形状

$$(1)\qquad \frac{f(t_1,\cdots,t_n)}{g(t_1,\cdots,t_n)},\ g(t_1,\cdots,t_n)\neq 0,$$

这里$f,g\in F[X_1,\cdots,X_n]$。这样的元素都属于$F(t_1,\cdots,t_n)$。另一方面，K中一切形如(1)的元素已经作成一个既包含F又包含$t_1,\cdots,t_n$的子域。这就证明了(iii)成立。 ∎

域F的扩域K可以看成F上一个向量空间。如果K在F上的维数是有限的，那么就称K是F的一个有限次扩域或者称K/F是一个有限次扩域。如果K是F上无限维的向量空间，就称K是F的一个无限次扩域，相应地，称K/F是一个无限次扩张。作为向量空间，K在F上的维数叫做K在F上的次数，记作$[K:F]$，向量空间K在F上的基也称为域K在F上的基。

定理 1.1.2 设E是域扩张K/F的一个中间域。$\{u_\alpha\}_{\alpha\in I}$是$E$在$F$上的一个基而$\{v_\beta\}_{\beta\in J}$是$K$在$E$上的一个基。那么$\{u_\alpha v_\beta\}_{\alpha\in I,\beta\in J}$是$K$在$F$上的一个基。

证 首先$\{u_\alpha v_\beta\}_{\alpha\in I,\ \beta\in J}$里任意有限个元素$\{u_i v_j\}_{1\leqslant i\leqslant m,\ 1\leqslant j\leqslant n}$在$F$上线性无关。事实上，如果有$a_{ij}\in F$，$1\leqslant i\leqslant m$，$1\leqslant j\leqslant n$．使得

$$\sum_{i=1}^{m}\sum_{j=1}^{n}a_{ij}u_iv_j=0,$$

则

$$\sum_{j=1}^{n}\left(\sum_{i=1}^{m}a_{ij}u_i\right)v_j=0.$$

$\sum_{i=1}^{m}a_{ij}u_i\in E$，$1\leqslant j\leqslant n$，而$v_1,\cdots,v_n$在$E$上线性无关，所以

$$\sum_{i=1}^{m} a_{ij}u_i = 0, \quad 1 \leqslant j \leqslant n.$$

又因为$u_1, \cdots, u_m$在F上线性无关，所以 $a_{ij}=0$，$1 \leqslant i \leqslant m$，$1 \leqslant j \leqslant n$.

其次，设$u \in K$，那么 u 可以由$\{u_\beta\}_{\beta \in J}$中有限个元素$v_1, \cdots, v_n$线性表示，系数属于$E$：

$$u = \sum_{j=1}^{n} b_j v_j, b_j \in E \,(1 \leqslant j \leqslant n).$$

每一个b_j又可以表成$\{u_\alpha\}_{\alpha \in I}$中有限元素的$F$-线性组合。因此存在$u_1, \cdots, u_m \in \{u_\alpha\}_{\alpha \in I}$，使得

$$b_j = \sum_{i=1}^{m} a_{ij}u_i, a_{ij} \in F (1 \leqslant i \leqslant m, 1 \leqslant j \leqslant n).$$

于是

$$u = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij}u_i v_j.$$

所以 u 可以表成$\{u_\alpha v_\beta\}_{\alpha \in I, \beta \in J}$中有限个元素的 F-线性组合。这就证明了$\{u_\alpha v_\beta\}_{\alpha \in I, \beta \in J}$是$K$在$F$上的一个基。 ▌

由这个定理，我们立即得到以下

推论 1.1.3 设 K/F 是一个有限次域扩张，而

$$E_1 \subseteq E_2 \subseteq \cdots \subseteq E_s$$

都是K/F的中间域。那么

$$[K:F] = [K:E_s][E_s:E_{s-1}]\cdots[E_1:F].$$ ▌

1.2 素域

如果一个域没有真子域，就称为一个素域。

有理数域$\mathbf{Q}$显然是一个素域。设$\mathbf{Z}$是整数环，p是一个素数。令

$$(p) = \{pn \mid n \in \mathrm{Z}\}$$

是 p 所生成的Z的理想。我们知道，以 p 为模的剩余类环 $Z/(p)$ 是一个域并且也是素域。

下面的定理对素域作了完全的描述。

定理 1.2.1 令 F 是一个素域。那么 F 或者与有理数域Q同构，或者与以某一个素数 p 为模的剩余类环同构。

证 令 1 是素域 F 的单位元，映射

$$\varphi: Z\to F,\quad n\to n\cdot 1$$

是一个环同态。令 $\mathfrak{p}=\ker\varphi$ 是 φ 的核。则 $\mathfrak{p}$ 是Z的一个理想，且

$$Z/\mathfrak{p}\cong\varphi(Z)\subseteq F.$$

因为 $\varphi(1)\neq 0$，所以 $\mathfrak{p}\neq Z$。由于 $\varphi(Z)$ 是整环，而Z是主理想环，因此，或者 $\mathfrak{p}=(0)$，或者 $\mathfrak{p}=(p)$，这里 (p) 是由某一个素数 p 所生成的 Z 的理想。

如果 $\mathfrak{p}=(0)$，那么 φ 是单射，并且可以开拓为Z的商域Q到 F 的单射，$\varphi(Q)$ 是 F 的子域。因为 F 是素域，所以 $\varphi(Q)=F$。这样，$Q\cong F$。

如果 $\mathfrak{p}=(p)$，那么 $Z/\mathfrak{p}=Z/(p)$ 是域，从而 $\varphi(Z)$ 是 F 的子域。因为 F 是素域，所以 $\varphi(Z)=F$，这样就得到 $Z/(p)\cong F$。 ∎

设 F 是任意一个域。F 的一切子域的交 F_0 仍是 F 的一个子域。F_0 显然是 F 的最小子域，所以 F_0 是一个素域，称为域 F 的素域。由1.2.1知，或者 $F_0\cong Q$，或者 $F_0\cong Z/(p)$，p 是一个素数。在前一情形，就说 F **具有特征零**；在后一情形，就说 F **具有特征** p。我们把域 F 的特征记作 char F。下面两个定理是比较显易的，我们把它们的证明留给读者去作。

定理 1.2.2 设 F 是一个域。

(i) 如果 $\mathrm{char}\ F=0$，那么对于 $n\in Z$，$x\in F$，

$$nx=0\Longleftrightarrow x=0 \text{ 或 } n=0.$$

(ii) 如果 $\mathrm{char}\ F=p>0$，那么对于 $n\in Z$，$x\in F$，

$$nx=0\Longleftrightarrow x=0 \text{ 或 } n\equiv 0\ (\mathrm{mod.}\ p).$$ ∎

定理 1.2.3 设F是一个域，$\mathrm{char}F=p>0$。那么对于任意$x,y\in F$和任意非负整数n，

（i） $(x\pm y)^{p^n}=x^{p^n}+y^{p^n}$；

（ii） 映射φ：$x\longmapsto x^{p^n}$是F到自身内的同态单射。 ▮

1.3 单扩域

设F是一个域，添加一个元素α于F所得的扩域$F(\alpha)$叫做F的一个**单扩域**。

单扩域的结构和所添加的元素α的性质有着密切的关系，先引入以下的概念。

设R是一个有单位元1的交换环，F是R的一个子域且F含有R的单位元。R的一个元素α称为**关于F是代数的**或者说α是F上一个**代数元**，如果存在F上一个非零多项式$f(X)$，使得$f(\alpha)=0$，如果α不是F上的代数元，就称α**关于F是超越的**或者说α是F上一个**超越元**。

设K是R的一个子域，且$F\subseteq K$。如果$\alpha\in R$关于F是代数的，那么显然α关于K也是代数的。一个等价的提法是，如果α关于K是超越的，那么α关于F也是超越的。

单扩域的结构由下面的定理完全决定。

定理 1.3.1 设$K=F(\alpha)$是域F的一个单扩域。

（i） 如果α关于F是超越的，那么K与F上不定元X的有理分式域$F(X)$同构。

（ii） 如果α关于F是代数的，那么存在F上一个最高次项系数是1的不可约多项式$p(X)$。而K与剩余类环$F[X]/(p(X))$同构，这里$(p(X))$表示由多项式$p(X)$所生的$F[X]$的理想；这个多项式$p(X)$由α唯一确定。

证 对于每一个$f(X)\in F[X]$，令$f(\alpha)\in K$与它对应，这

样就定义了一个环同态φ：$F[X]\to K$，并且φ保持F的元素不动．$\varphi(F[X])=F[\alpha]$是K的一个子整环．令

$$\mathfrak{p}=\mathrm{Ker}\,\varphi=\{f(X)\mid f(X)\in F[X],\ f(\alpha)=0\}.$$

$\mathfrak{p}$是环$F[X]$的一个理想．

（i） 如果α关于F是超越的，那么不存在非零多项式$f(X)\in F[X]$使$f(\alpha)=0$，从而$\mathfrak{p}=(0)$．所以φ是$F[X]$到$F[\alpha]$的同构映射，这个映射可以开拓为有理分式域$F(X)$到整环$F[\alpha]$的商域$F(\alpha)$的同构映射，仍以φ表示：

$$\varphi:\frac{f(X)}{g(X)}\longmapsto\frac{f(\alpha)}{g(\alpha)}.$$

这样，φ是$F(X)$到K同构映射，且$\varphi(X)=\alpha$．

（ii） 设α关于F是代数的，那么存在$F[X]$的非零多项式$f(X)$，使得$f(\alpha)=0$，所以$\mathfrak{p}\neq(0)$．由于$F[X]$是欧氏环，所以$\mathfrak{p}$由一个多项式$p(X)\neq 0$生成：$\mathfrak{p}=(p(X))$，$p(X)$是使$p(\alpha)=0$的非零多项式中次数最低的一个．不妨设$p(X)$的最高次项系数等于1，于是$p(X)$由α唯一确定，并且容易看出，$p(X)$是不可约的．于是$\mathfrak{p}=(p(X))$是$F[X]$的一个极大理想，从而剩余类环$F[X]/\mathfrak{p}$是一个域，于是就有

$$F[X]/\mathfrak{p}\cong\varphi(F[X])=F[\alpha]\subseteq K.$$

因此$F[\alpha]$也是域，然而$K=F(\alpha)$是含有F及α的最小域，所以

$$F(\alpha)=F[\alpha]，即$$

$$F[X]/\mathfrak{p}\cong K. \qquad \blacksquare$$

定理 1.3.1 完全给出了一个域F的单扩域$F(\alpha)$的结构，当α是F上的代数元时，我们还可以说得更具体一些．首先，由1.3.1，当α是F上代数元时，存在唯一的最高次项系数是1的不可约多项式$p(X)\in F[X]$，使得$p(\alpha)=0$．我们把这个由α所唯一确定的多项式$p(X)$叫做α在F上的**最小多项式**．我们有

定理 1.3.2 设α是域F上一个代数元，$p(X)\in F[X]$是α在F上的最小多项式，设$\deg\ p(X)=n$。

(i) 元素$1,\alpha,\cdots,\alpha^{n-1}$构成$F(\alpha)$在$F$上的一个基，从而$F(\alpha)$的每一元素$\xi$可以唯一地表示成

$$\xi=a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1},a_i\in F(0\leqslant i\leqslant n-1),$$

的形式。$[F(\alpha):F]=\deg\ p(X)$。

(ii) 设 $\xi=\sum_{i=0}^{n-1}a_i\alpha^i$，$\eta=\sum_{i=0}^{n-1}b_i\alpha^i\in F(\alpha)$，那么

$$\xi+\eta=\sum_{i=0}^{n-1}(a_i+b_i)\alpha^i$$

(iii) 令 $f(X)=\sum_{i=0}^{n-1}a_iX^i$，$g(X)=\sum_{i=0}^{n-1}b_iX^i$ 而

$$r(X)=c_0+c_1X+\cdots+c_{n-1}X^{n-1}$$

是以$p(X)$除$f(X)g(X)$所得的余式，则

$$\xi\eta=\sum_{i=1}^{n-1}c_i\alpha^i.$$

证 由1.3.1，对于$K=F(\alpha)=F[\alpha]$的任意元素，存在$f(X)\in F[X]$，使得$\xi=f(\alpha)$。设

$$f(X)=p(X)q(X)+r(X),$$

这里或者$r(X)=0$，或者$\deg r(X)<n$，那么

$$\xi=f(\alpha)=r(\alpha).$$

因此

$$\xi=a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1},a_i\in F(0\leqslant i\leqslant n-1).$$

这个表示法是唯一的，因为如果

$$\xi=\sum_{i=0}^{n-1}a_i\alpha^i=\sum_{i=0}^{n-1}a_i'\alpha^i,\quad a_i,a_i'\in F,$$

那么令$g(X)=\sum_{i=0}^{n-1}(a_i-a_i')X^i\in F[X]$，则$g(\alpha)=0$，所以$p(X)$整除$g(X)$，从而必须$g(X)=0$，这样就证明了，$1,\alpha,\cdots,\alpha^{n-1}$是

$F(\alpha)$ 在 F 上的一个基，从而$[F(\alpha):F]=n$。至于论断(ii)和(iii)是显然的。 ▮

由以上两个定理立即得到

推论1.3.3 设$K=F(\alpha)$是域F的一个单扩域。K是F上有限次扩域必要且只要α关于F是代数的。 ▮

因为域F上不定元是存在的，所以由1.3.1(i)可知，域F上添加一个超越元的单扩域是存在的。下面的定理表明，域F上添加一个代数元的单扩也是存在的。

定理 1.3.4 设$p(X)\in F[X]$是域F上不定元X的一个不可约多项式。那么存在F的一个扩域K，使得$p(X)$在K内有一个根α，并且$K=F(\alpha)$。

证 令$\mathfrak{p}=(p(X))$是$p(X)$所生成的$F[X]$理想。由于$p(X)$不可约，所以$\mathfrak{p}$是一个极大理想。令$K=F[X]/\mathfrak{p}$，则K是一个域。因为$F\cap\mathfrak{p}=\{0\}$，所以自然同态$\varphi: F[X]\to K$将F单一地映入K，从而可以将$\varphi(F)$与F等同，而将F看成K的一个子域。令$\alpha=\varphi(X)\in K$，对于任意$g(X)\in F[X]$，我们有

$$\varphi(g(X))=g(\varphi(X))=g(\alpha).$$

所以$K=\varphi(F[X])=\{g(\alpha)\mid g(X)\in F[X]\}=F[\alpha]$，然而$K$是域，所以$K=F[\alpha]=F(\alpha)$。 ▮

习　题

1. 设K是域F的一个有限次扩域，证明：

(i) $[K:F]=1\Longleftrightarrow K=F$；

(ii) 如果$[K:F]=p$是一个素数，则在F与K之间没有不等于F或K的中间域；

(iii) 如果$\alpha\in K$是F上一个n次代数元，则$n\mid[K:F]$。

2. 设$K=\mathbf{Q}(\sqrt{2},\sqrt{3})$。求出$[K:\mathbf{Q}]$，并且给出$K$在$\mathbf{Q}$上一个基。

3. 设F是一个素域，$F(X_1, X_2)$是F上不相关不定元X_1, X_2的有理分式域．试给出F的一个扩域K及$u, v \in K$，使得u, v都是F上超越元，但$F(u, v) \neq F(X_1, X_2)$．

4. 证明，$\mathbf{Q}(\sqrt{2})$和$\mathbf{Q}(\sqrt{-1})$作为$\mathbf{Q}$上的向量空间是同构的，但作为域则不同构．

4. 证明定理1.2.2.和1.2.3.

6. 设$F(\alpha)$是域F上一单扩域．证明，如果$[F(\alpha) : F]$是一个奇数，则$F(\alpha) = F(\alpha^2)$．

7. 设K是域F一个扩域，$\alpha \in K$．证明下列三个条件是等价的：

(i) α是F上的代数元；

(ii) 多项式环$F[\alpha]$是K的子域；

(iii) $F[\alpha]$是F上有限维向量空间．

8. 设α, β是域F的某一个扩域内的元素，$[F(\alpha) : F] = m$, $[F(\beta) : F] = n$，证明，$[F(\alpha, \beta) : F(\beta)] = m \Longleftrightarrow [F(\alpha, \beta) : F(\alpha)] = n$．

9. 设$X^n - a$是域F上一个多项式，α是$X^n - a$在F的某个扩域K内的一个根，$[F(\alpha) : F] = n$．令m是n的一个约数．证明$[F(\alpha^m) : F] = n/m$, $[F(\alpha) : F(\alpha^m)] = m$．

10. 设α是域F上一个代数元，$f(X)$是α在F上的最小多项式，设$a \in F$．证明$\alpha + a$在F上的最小多项式是$f(X - a)$．

11. 设K是域F的一个扩域，$u, v \in K$，其中v关于F是超越的，而关于$F(u)$是代数的．证明，u关于$F(v)$是代数的．

12. 令$F = \mathbf{Z}/(2)$是二元域．找出F上一个二次不可约多项式$f(X)$，并且添加$f(X)$的一个根α于F，得到一个四元域$F(\alpha)$．

用同样的方法构造一个F上的八元扩域K．写出这八个元素，并且证明它们正好是$X^8 - X$在K内的全部根．

13. 令$F(X)$是域F上不定元X的有理分式域，$u =$

$X^3/X+1$。证明$F(X)$是$F(u)$上的单扩域，并且求出$[F(X):F(u)]$。

14. 设α是域F上一个代数元，证明，对于$f(X)\in F[X]$来说，下列三个条件是等价的：

(i) $f(X)$是α在F上最小多项式；

(ii) $f(X)$是一个最高次项系数为1的多项式，并且满足条件：对于任意$g(X)\in F[X]$来说，$g(\alpha)=0 \Longleftrightarrow f(X)|g(X)$。

(iii) $f(X)$是一个最高次项系数为1的多项式，$f(\alpha)=0$。并且对于任意$0\neq g(X)\in F[X]$来说，若$g(\alpha)=0$，则

$$\deg f<\deg g.$$

15. 设$f(X)=X^4+aX^2+b^2$是有理数域$\mathbf{Q}$上一个不可约多项式，θ是$f(X)$在复数域内一个根。证明，$K=\mathbf{Q}(\theta)$恰含有三个在$\mathbf{Q}$上是二次的子域。

16. 设F是一个特征不等于2的域，α,β分别是F上不可约多项式X^2-a和X^2-b在F的某一个扩域内的根，证明，$F(\alpha)=F(\beta)\Longleftrightarrow a=bc^2, c\in F$。

17. 设$\alpha\in\mathbf{C}$是有理数域$\mathbf{Q}$上多项式X^3-X^2+X+2的一个根。将$(\alpha^2+\alpha+1)(\alpha^2-\alpha)$和$(\alpha-1)^{-1}$表成$a\alpha^2+b\alpha+c$ $(a, b, c\in\mathbf{Q})$的形式。

18. (Eisenstein判断法)，设R是一个唯一分解整环，$R[X]$是R上不定元X的多项式环。设

$$f(X)=a_0X^n+a_1X^{n-1}+\cdots+a_{n-1}X+a_n\in R[X].$$

如果存在R中一个素元p，使得：(i)$p\nmid a_0$；(ii)$p|a_i$，$1\leqslant i\leqslant n$；(iii)$p^2\nmid a_n$，则$f(X)$不能分解成为$R[X]$中两个次数都低于n的多项式的乘积。

〔注：这个事实在以后的讨论中有时被用到，证明时并不用域的知识。〕

第二章　代数扩张

我们已经看到，域F的一个扩域K的元素可以分成两类，一类是F上的代数元，另一类是F上的超越元。如果K中每一个元素都是F上的代数元，那么K就叫做F的一个代数扩域。代数扩域是一种非常重要的扩域。在这一章里，我们将讨论这种扩域的一些基本性质。

2.1　代数扩域

设K是域F的一个扩域。如果K的每一元素都是F上的代数元，就称K是F的一个**代数扩域**，这时K/F称为一个**代数扩张**；在相反的情形，也就是说，如果K中存在F上的超越元，就称K是F的一个**超越扩域**，而K/F称为一个**超越扩张**。

引理 2.1.1　设$K = F(\alpha_1, \cdots, \alpha_n)$是域$F$的一个有限生成的扩域，而$\alpha_1, \cdots, \alpha_n$都是$F$上代数元。那么$K$是$F$上有限次扩域，并且

$K = F[\alpha_1, \cdots, \alpha_n] = \{f(\alpha_1, \cdots, \alpha_n) \mid f(X_1, \cdots, X_n) \in F[X_1, \cdots, X_n]\}$，$X_1, \cdots, X_n$是$F$上不相关不定元。

证　对生成元的个数n作归纳法。$n = 1$时，$K = F(\alpha_1)$，α_1是F上代数元。由1.3.2(i)，K是F的有限次扩域，并且$K = F[\alpha_1]$。

设　$n > 1$，并且假设对于$n-1$来说，定理成立，现在设$K = F(\alpha_1, \cdots, \alpha_n)$，$\alpha_1, \cdots, \alpha_n$是$F$上代数元。令$K' = F(\alpha_1, \cdots, \alpha_{n-1})$。则$K = K'(\alpha_n)$，$F \subseteq K' \subseteq K$。由归纳法假设，$[K' : F] < \infty$且$K' = F[\alpha_1, \cdots, \alpha_{n-1}]$；又$[K : K'] < \infty$，所以

$$[K:F]=[K:K'][K':F]<\infty,$$

并且

$$K=K'[\alpha_n]=F[\alpha_1,\cdots,\alpha_{n-1}][\alpha_n]=F[\alpha_1,\cdots,\alpha_n]. \blacksquare$$

定理 2.1.2 设K是域F的一个扩域．对于K来说，以下两个条件是等价的：

（i） K是F上有限次扩域；

（ii） K是F上有限生成的代数扩域．

证 (i)$\Longrightarrow$(ii)．设$[K:F]<\infty$．令α是K中任意元素．则$F(\alpha)\subseteq K$，从而

$$[F(\alpha):F]\leqslant[K:F]<\infty,$$

所以由1.3.3，α是F上代数元．因此K/F是代数扩张．令α_1，$\cdots$，$\alpha_n\in K$是K在F上的一个基．则$K=F(\alpha_1,\cdots,\alpha_n)$．

(ii)$\Longrightarrow$(i) 由2.1.1． $\blacksquare$

定理 2.1.3 设L是域F的一个扩域，S是L的一个子集，并且S的每一个元素都是F上代数元．那么$K=F(S)$是F的一个代数扩域；K中每一元素ξ可以表成以下形式的有限项的和：

$$\xi=\sum a_{k_1\dots k_m}\alpha_1^{k_1}\cdots\alpha_m^{k_m},$$

这里$\alpha_1,\cdots,\alpha_m\in S$(依赖于$\xi$)，$a_{k_1\dots k_m}\in F$，$k_i$是非负整数，$i=1$，$\cdots$，$m$．

证 令$\{S_\alpha\}$是S的有限子集族．由1.1.1 (ii)，$K=F(S)=\bigcup_\alpha F(S_\alpha)$，设$\xi\in K$．那么存在$S$的一个有限子集$S_\alpha=\{\alpha_1,\cdots,\alpha_m\}$．使得

$$\xi\in F(S_\alpha)=F(\alpha_1,\cdots,\alpha_m).$$

由2.1.1和2.1.2，$F(\alpha_1,\cdots,\alpha_m)$是$F$的代数扩域，所以$\xi$关于$F$是代数的．由于$\xi$是$K$任意元素，所以$K$是$F$的代数扩域，再由2.1.1．$\xi=f(\alpha_1,\cdots,\alpha_m)\in F[\alpha_1,\cdots,\alpha_m]$． $\blacksquare$

推论 2.1.4 设K是域F的一个扩域．$\alpha,\beta\in K$是F上代数元，那么$\alpha+\beta$，$\alpha-\beta$，$\alpha\beta$，$\alpha\beta^{-1}$（当$\beta\neq 0$时）都是F上代数元．

证 在2.1.3中，取$S=\{\alpha,\beta\}$，则$F(\alpha,\beta)$是F的代数扩域． ▮

定理 2.1.5 设K是域扩张L/F的一个中间域，即$F\subseteq K\subseteq L$．L/F是代数扩张必要且只要L/K和K/F都是代数扩张．

证 必要性是显然的．反之，设L/K和K/F都是代数扩张．设$\xi\in L$．因为ξ关于K是代数的，所以存在$K[X]$中非零多项式

$$g(X)=\sum_{j=0}^{n}a_jX^j,\ a_j\in K\ (0\leqslant j\leqslant n),$$

使得$g(\xi)=0$．又K关于F是代数的，所以$a_j(0\leqslant j\leqslant n)$是$F$上代数元．于是由2.1.1，$K'=F(a_0,a_1\cdots,a_n)$是$F$的有限次扩域，并且$g(X)\in K'[X]$．因此$\xi$关于$K'$是代数的，从而$[K'(\xi):K']<\infty$．这样，

$$[K'(\xi):F]=[K'(\xi):K'][K':F]<\infty.$$

再由2.1.1，$K'(\xi)$是F的代数扩域，因而ξ是F上代数元． ▮

推论 2.1.6 设

$$F=F_0\subseteq F_1\subseteq\cdots\subseteq F_n=K$$

是一个扩域序列，这里F_i是F_{i-1}的扩域$(1\leqslant j\leqslant n)$．那么$K/F$是代数扩张必要且只要每一$F_i/F_{i-1}$都是代数扩张$(1\leqslant j\leqslant n)$． ▮

设K和E都是一个域L的子域．L中包含K和E的最小子域叫做K与E的**合成域**，记作KE．显然

$$KE=K(E)=E(K).$$

定理 2.1.7 设L是F域的一个扩域，K和E都是L/F的中间域．

（i） 如果K是F的代数扩域，则KE是E的代数扩域．

（ii） 如果K和E都是F的代数扩域，则KE也是F的代数

扩域。

证 (i) $KE=E(K)$，而K的每一元素都是F上代数元，所以也都是E上代数元，由2.1.3 KE是E的代数扩域。

(ii) 由(i)，KE是E的代数扩域，而E又是F的代数扩域。由2.1.5，KE是F的代数扩域。 ▌

设K是域F的一个扩域。令A是K中在F上的代数元的全体。由2.1.4，A是K的一个子域，且$F\subseteq A\subseteq K$。子域A叫做F在K中的**代数闭包**。特别当$F=A$的，就说F在K中是**代数闭的**。

例如，有理数域Q在复数域C中的代数闭包就是代数数的全体。

定理 2.1.8 设K是域F的一个扩域，A是F在K中的代数闭包。则A在K中是代数闭的。

证 令A'是A在K中的代数闭包。我们有以下的一串扩域

$$F\subseteq A\subseteq A'\subseteq K.$$

A/F, A'/A都是代数扩张，由2.1.5，A'/F是代数扩张。但A是F在K中的代数闭包，所以$A'\subseteq A$，从而$A'=A$。 ▌

定理 2.1.9 设$X_1,\cdots,X_n$是域F上不相关不定元，$K=F(X_1,\cdots,X_n)$是F上$X_1,\cdots,X_n$的有理分式域。那么F在K中是代数闭的。

证 对n作数学归纳法。

$n=1$时，$K=F(X)$，X是F上不定元。设$\alpha\in K$，则

$$\alpha=f(X)/g(X),\ f(X),g(X)\in F[X],\ g(X)\neq 0.$$

设α关于F是代数的。如果$\alpha\notin F$。考虑域$F(\alpha)$上不定元T的多项式$f(T)-\alpha g(T)$。则

$$f(T)-\alpha g(T)\neq 0.$$

事实上，如果$f(T)-\alpha g(T)=0$，那么在$f(T)-\alpha g(T)$中，T的系数都是零。然而这些系数都是α的一次多项式，系数属于F，

由此就得出$\alpha\in F$的结论．这就导致矛盾．这样一来，X是$F(\alpha)$上非零多项式$f(T)-\alpha g(T)$的根，从而X关于$F(\alpha)$是代数的．又$F(\alpha)$是F的代数扩域，所以X是F上代数元．这又导致矛盾．因此必须$\alpha\in F$，F在K中代数闭．

现在设$n>1$并且假设对于$n-1$来说，定理成立．令$F'=F(X,\cdots,X_{n-1})$，则$K=F'(X_n)$，设$\alpha\in K$关于F是代数的．那么α关于F'也是代数的，由上面所证的$n=1$的情形，F'在K中代数闭，所以$\alpha\in F'$．再由归纳法的假设，$\alpha\in F$．所以F在K中是代数闭的． ▌

习　题

1. 设K和L都是域扩张M/F的中间域．令$R=\{\sum_i x_iy_i$（有限和）$|x_i\in K, y_i\in L\}$．证明：

（i） R是M中包含K及L的一个子整环；

（ii） 合成域KL是R的商域；

（iii） 如果K或L是F的代数扩张，则$R=KL$．

2. 设K是域F的一个扩域．证明，K是F的代数扩域必要且只要任意满足条件$F\subseteq A\subseteq K$的子整环A都是子域．

3. 设F_1,F_2都是域K的子域，S是K的一个子集．证明，如果F_1的每一个元素都是F_2上的代数元，则$F_1(S)$的每一个元素都是$F_2(S)$上的代数元．

4. 设K和L都是域扩张M/F的中间域．证明：

(i) $[KL:F]$是有限的必要且只要$[K:F]$和$[L:F]$都是有限的；

(ii) 如果$[KL:F]$是有限的，则$[K:F]$与$[L:F]$都整除$[KL:F]$，且$[KL:F]\leqslant[K:F][L:F]$；

(iii) 如果$[K:F]$与$[L:F]$都是有限的且互素，则$[KL:L]=[K:F]$．

5. 设K和L都是域扩张M/F的中间域且K和L都是F的有限次扩域。

(i) 证明，如果$[KL:F]=[K:F][L:F]$，则$K\cap L=F$。

(ii) 证明，如果$[K:F]$或$[L:F]$等于2，那么(i)的逆命题也成立。

(iii) 举一反例说明，(i)的逆命题一般不成立。

6. 设K是域F的一个有限次扩域．证明，如果对于K/F的任意两个中间域E_1,E_2来说，要么$E_1\subseteq E_2$，要么$E_2\subseteq E_1$，则K是F的一个单扩域。

7. 设F是一个域且char $F\neq 2$．α,β分别是$F[X]$中不可约多项式X^2-a和X^2-b在F的某一个扩域内的根．证明，$F(\alpha,\beta)=F(\alpha(\beta+1))$。

8. 设F是一个域且char$F\neq 2$，K是F的一个四次扩域．证明，以下两个条件是等价的：

(i) 存在K/F的一个中间域E，使得$[E:F]=2$；

(ii) $K=F(\theta)$，θ是$F[X]$中一个形如X^4+aX^2+b的不可约多项式的根。

9. 设α是域F上不可约多项式X^2-X-a的一个根．证明，对于$K=F(\alpha)$的元素β来说，以下两个条件是等价的：

(i) β是$F[X]$中一个形如X^2-X-b的不可约多项式的根；

(ii) $\beta=c+(1-2c)\alpha$，其中$c\in F$，$2c\neq 1$．

10. 设K是F域的一个代数扩域，$N^+=\{1,2,3,\cdots\}$是一切自然数所成的集．证明：

(i) 存在K到$F[X]\times N^+=\{(f,i)\mid f\in F[X],i\in N^+\}$内的一个单射；

(ii) 如果F是有限域，则K的基数是至多可数的；

(iii) 如果F是无限域，则K与F有相同的基数。

2.2 代数闭包

在这一节里，我们要引进一个域的代数闭包的概念，并且证明，在同构的意义下，每一个域恰有一个代数闭包。

引理2.2.1 设F是一个域．$f_i(X)\in F[X]$，$1\leqslant i\leqslant n$，是F上任意n个非常数多项式．那么存在F的一个扩域K使得每一个$f_i(X)$在K中有一个根．

证 当$n=1$时，令$p(X)$是$f_i(X)$的一个不可约因式．由1.3.4，存在F的扩域K，使$p(X)$在K内有一个根α，从而$f(\alpha)=0$．

设 $n>1$，并且设对于$n-1$来说引理成立，于是存在F一个扩域K'，使得$f_i(X),\cdots,f_{n-1}(X)$在K'内各有一个根．然而$f_n(X)\in F[X]\subseteq K'[X]$，所以存在$K'$的一个扩域$K$，使得$f_n(X)$在$K$内有一个根，从而$f_1(X),\cdots,f_n(X)$在$K$内各有一个根． ∎

现在引入一个域的代数闭包的概念．先引入代数闭域的概念．

一个域K说是**代数闭的**，如果$K[X]$中每一次数大于零的多项式在K中有一个根．

定义 域F的一个扩域Ω叫做F的一个代数闭包，如果

(i) Ω是F的代数扩域；

(ii) Ω是代数闭域．

定理 2.2.2 设K是域F的一个扩域，A是F在K内的代数闭包．如果K是代数闭域，则A是F的一个代数闭包．

证 因为A是K中在F上的代数元的全体，所以A是F的代数扩域．我们证明，A是代数闭的．设$g(X)\in A[X]$是一个次数大于零的多项式．因为K是代数闭域，所以$g(X)$在K内有一个根α．α关于A是代数的，而由定理2.1.8，A在K中是代数

闭的，所以$\alpha \in A$。这就证明了A是代数闭域。 ∎

定理 2.2.3 任意域F都有一个代数闭包。

证 证明分两步。先证存在F的一个代数扩域，使得$F[X]$每一个次数大于零的多项式在这个扩域里有一个根。然后从F出发，作一个串扩域

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots$$

使得F_{i+1}是F_i的代数扩域，并且$F_i[X]$中每一个次数大于零的多项式在F_{i+1}内有一个根（$i = 0, 1, 2, \cdots$）。令$\Omega = \bigcup_{i=0}^{\infty} F_i$。证明$\Omega$就是$F$的一个代数闭包。

先证第一步。证明的思想与证明一个多项式的根的存在（定理1.3.4）类似。考虑$F[X]$中一切次数大于零的多项式的集

$$F[X] \setminus F = \{f_\lambda(X) \mid \lambda \in \Lambda\},$$

这里Λ是与$F[X] \setminus F$有相同基数的一个指标集。对于每一个$\lambda \in \Lambda$，令一个符号X_λ与它对应，将$\{X_\lambda\}_{\lambda \in \Lambda}$看成$F$上不相关不定元，即$\{X_\lambda\}_{\lambda \in \Lambda}$的任意有限子集都是$F$上不相关不定元。令$R = F[\{X_\lambda\}_{\lambda \in \Lambda}]$表示$\{X_\lambda\}_{\lambda \in \Lambda}$的一切有限子集在$F$上所生成的多项式环的并集。$R$里每一个元素都是有限个不定元$X_{\lambda_1}, \cdots, X_{\lambda_n} \in \{X_\lambda\}_{\lambda \in \Lambda}$在$F$上的多项式。这样定义的$R$的元素是无歧义的。显然，一切$f_\lambda(X_\lambda) \in R (\lambda \in \Lambda)$。

令$\mathfrak{a}$是由一切$f_\lambda(X_\lambda)$，$\lambda \in \Lambda$，所生的R的理想。因为R是有单位元的交换环，所以$\mathfrak{a}$的元素都有以下形状：

$$\sum_k u_k f_k(X_k) \quad （有限和）, \tag{1}$$

这里u_k是有限个$X_\lambda(\lambda \in \Lambda)$的多项式。$\mathfrak{a}$是$R$的一个真子集，因为不然的话，将有$1 \in \mathfrak{a}$，从而可以表成(1)的形式：

$$1 = \sum_k u_k f_k(X_k).$$

右端只有有限个$f_k(X_k)$出现，所以由2.2.1，存在F的一个扩

域，使每一个$f_k(X_k)$在这个扩域中有一个根α_k，代入上式得出矛盾的等式$1=0$。

这样，存在R的一个极大理想．$\mathfrak{m}\supseteq\mathfrak{a}$。令$F_1=R/\mathfrak{m}$，则$F_1$是一个域．令

$$\varphi: R\to F_1=R/\mathfrak{m}$$

是自然同态．因为$F\cap\mathfrak{m}=\{0\}$，所以$\varphi|_F$是单射，因而可以把$\varphi(F)$与F等同起来，而F可以认为是F_1的一个子域．

F_1是F的代数扩域．事实上，设$x_\lambda=\varphi(X_\lambda)$，则$F_1$是由$\{x_\lambda\}_{\lambda\in\Lambda}$在$F$上生成的域．另一方面，对于每一个$\lambda\in\Lambda$，$f_\lambda(X_\lambda)\in\mathfrak{a}\subseteq\mathfrak{m}$。所以$f_\lambda(x_\lambda)=\varphi(f_\lambda(X_\lambda))=0$。因此$x_\lambda$是$F$上代数元．由2.1.3，$F_1$是$F$的代数扩域．

由于F_1是由一切$f_\lambda(X_\lambda)$的根x_λ在F上生成的，这就证明了，存在F的代数扩域F_1，使得$F[X]$的每一个次数>0的多项式$f(X)$在F_1中有一个根．

这样，我们可以归纳地构造出一个扩域序列

$$F=F_0\subseteq F_1\subseteq\cdots\subseteq F_i\subseteq F_{i+1}\subseteq\cdots,$$

使得

1° F_{i+1}是F_i的代数扩域；

2° $F_i[X]$的每一个次数>0的多项式在F_{i+1}内有一个根，$i=0,1,2,\cdots$。

令$\Omega=\bigcup_{i=0}^{\infty}F_i$，容易证明，$\Omega$是一个域．我们证明，$\Omega$是$F$的一个代数闭包．

首先，Ω是F代数扩域．设$\alpha\in\Omega$，那么存在i，使得$\alpha\in F_i$，F_i是F的代数扩域，所以α是F上的代数元．

其次，Ω是代数闭的．设

$$f(X)=a_0+a_1X+\cdots+a_nX^n\in\Omega[X],$$

$n>0$，$a_i\in\Omega$，$i=0,1,\cdots,n$。于是存在一个整数$k>0$，

使得 $a_i\in F_k$，$i=0, 1, \cdots, n$。$f(X)\in F_k[X]$，所以 $f(X)$ 在 F_{k+1} 内有一个根，因而在 Ω 内有一个根。

这就证明了 Ω 是 F 的代数闭包。 ∎

定理 2.2.4 设 $\varphi: F\to F'$ 是域 F 到域 F' 的一个同构映射，Ω 和 Ω' 各是 F 和 F' 的一个代数闭包。那么 φ 可以开拓为 Ω 到 Ω' 的同构，即存在域同构 $\psi: \Omega\to\Omega'$，使得 $\psi|_F=\varphi$。

特别，一个域 F 的任意两个代数闭包都是同构的。

证 显然，取 $F'=F$，φ 是 F 的恒等的同构，则最后论断可以由前一个论断直接得出。因此只要证明前一论断。设 K 是域扩张的一个中间域。令 ψ 是 φ 到 K 上的一个开拓，即 $\psi: K\to\Omega'$ 是一个单同态并且 $\psi|_F=\varphi$。考虑一切这样的对 (K, ψ) 所成的集 S。S 不空，因为 $(F, \varphi)\in S$。对于 S 中任意两个元素 (K_1, ψ_1)，(K_2, ψ_2)，规定，

$$(K_1, \psi_1)\leqslant(K_2, \psi_2)，\text{如果 } K_1\subseteq K_2 \text{ 且 } \psi_2|_{K_1}=\psi_1。$$

这样一来，S 作成一个偏序集。我们证明，S 是一个归纳集。设

$$S'=\{(K_\lambda, \psi_\lambda)\mid\lambda\in\Lambda\}$$

是 S 的一个非空链，令

$$K=\bigcup_{\lambda\in\Lambda}K_\lambda.$$

K 显然是 Ω 的一个子域。设 $\alpha\in K$，那么 α 属于某一 $K_\lambda, \lambda\in\Lambda$，因此，对于任意 $\mu\in\Lambda$，如果 $K_\lambda\subseteq K_\mu$，则 $\alpha\in K_\mu$，我们如下地定义 $\psi: K\to\Omega'$。如果 $\alpha\in K_\lambda$，则定义 $\psi(\alpha)=\psi_\lambda(\alpha)$。因为当 $K_\lambda\subseteq K_\mu$ 时，$\psi_\mu|_{K_\lambda}=\psi_\lambda$，所以这样定义是无歧义的，并且 ψ 是 K 到 Ω' 内的单同态。这样，$(K, \psi)\in S$。(K, ψ) 是 S' 的一个上界。于是由 Zorn 引理，S 有一个极大元素 (L, ω)。因为 Ω 是 F 的代数扩域，所以 Ω 也是 L 的代数扩域。

我们证明，$L=\Omega$。且 $\omega(L)=\omega(\Omega)=\Omega'$。

设 $\alpha\in\Omega$，令 $p(X)\in L[X]$ 是 α 在 L 上的最小多项式。令 $L'=\omega(L)\subseteq\Omega'$. ω 可以通过自然的方式开拓为环同构 $L[X]\to L'[X]$，我们仍用 ω 表示这个环同构。对于 $f(X)\in L[X]$，$\omega(f(X))$ 就是把 $f(X)$ 的系数 a_i 相应地换成 $\omega(a_i)$ 所得的 L' 上的多项式。因为 $p(X)$ 是 $L[X]$ 中不可约多项式，容易证明 $p'(X)=\omega(p(X))$ 是 $L'[X]$ 中不可约多项式。因此，剩余类环 $L[X]/(p(X))$ 和 $L'[X]/(p'(X))$ 都是域，并且 ω 诱导出域同构

$$\overline{\omega}: L[X]/(p(X))\to L'[X]/(p'(X)).$$

因为 Ω' 是代数闭域，所以存在 $\alpha'\in\Omega'$，使得 $p'(\alpha')=0$. 因为 $p'(X)$ 是 $L'[X]$ 中最高次项系数是1的不可约多项式，所以 $p'(X)$ 就是 α' 在 L' 上的最小多项式。于是由1.3.1，分别存在域同构

$$\sigma: L(\alpha)\to L[X]/(p(X)) \text{和} \sigma': L'(\alpha')\to L'[X]/(p'(X))$$

$\sigma|_L=1_L$，且 $\sigma|_{L'}=1_{L'}$. 令

$$\tau=\sigma'^{-1}\circ\omega\circ\sigma,$$

则 $\tau: L(\alpha)\to L'(\alpha')\subseteq\Omega'$ 是 $L(\alpha)$ 到 Ω' 内的单同态。对于任意 $\xi\in L$，我们有 $\tau(\xi)=\omega(\xi)$. 所以 $(L(\alpha),\tau)\in S$ 并且 $(L,\omega)\leqslant(L(\alpha),\tau)$. 由 (L',ω) 的极大性得

$$L(\alpha)=L,\quad \tau=\omega$$

这样，Ω 的任意元都在 L 内，所以 $L=\Omega$.

设 $\Omega''=\omega(L)=\omega(\Omega)\subseteq\Omega'$. 则 Ω'' 是代数闭域而 Ω' 是 Ω'' 的代数扩域，所以 $\Omega''=\Omega'$，即 $\omega(\Omega)=\Omega'$. ∎

推论 2.2.5 设 Ω 是域 F 的一个代数闭包，而 K 是 F 的一个代数扩域. 则 L 与 Ω/F 的一个中间域同构.

证 令 Ω' 是 K 的一个代数闭包. 则 Ω' 也是 F 的一个代数闭包. 由2.2.4，存在域同构 $\sigma:\Omega'\to\Omega$. 且 $\sigma|_F$ 就是 F 的恒等自同构. 令 $E=\sigma(K)$. 则 E 是 Ω/F 的一个中间域. ∎

以下为了叙述简便起见，我们引进一个术语. 设 K 和 L 都是

域F的扩域。同态或同构映射$\varphi: K\to L$叫做一个F-同态或F-同构，如果$\varphi|_F$是F的恒等自同构。

推论 2.2.6 设Ω是域F的一个代数闭包，K是Ω/F的一个中间域，$\varphi: K\to\Omega$是一个F-单同态。那么φ总可以开拓成为Ω的一个F-自同构。

证 Ω是K和$\varphi(K)$的代数闭包。由**定理**2.2.4，存在Ω的一个F-自同构ω，使得$\omega|_K=\varphi$。 ▮

推论 2.2.7 设Ω是域F的一个代数闭包。对于Ω的元素α,β来说，以下两个条件是等价的：

（i） β是α在F上最小多项式$p(X)$的根；

（ii） 存在Ω的一个F-自同构ω，使得$\omega(\alpha)=\beta$。

证 (i)$\Longrightarrow$(ii) $p(X)$也是β在F上的最小多项式。因此，存在F-同构

$$\varphi=F(\alpha)\cong F[X]/(p(X))\cong F(\beta),$$

且$\varphi(\alpha)=\beta$。由2.2.6，φ可以开拓成为Ω的一个同构ω。

(ii)$\Longrightarrow$(i) 设存在Ω的一个F-自同构ω，使得$\omega(\alpha)=\beta$。于是

$$p(\beta)=p(\omega(\alpha))=\omega(p(\alpha))=0.$$ ▮

习　题

1. 设F是一个域。如果对于F的每一个扩域K来说，F的包含在K内的最大代数扩域就是F本身，则F是代数闭的。

2. 设L是域F的一个代数扩域。证明，对于L来说，下列三条件等价：

（i） L是F的代数闭包；

（ii） 对于F的任意一个代数扩域K来说，存在一个F-同态单射$\varphi: K\to L$；

（iii） 设$\sigma: F'\to F$是一个域同构。那么对于F'的每一个

代数扩域K'来说，σ可以开拓为域同态单射$K'\to L$。

3. 设K是域F的一个代数扩域。证明，如果$F[X]$中每一个次数大于零的多项式在$K[X]$内可以分解成一次因式的乘积，那么$K[X]$的每一个次数大于零的多项式在$K[X]$内也可以分解成一次因式的乘积。

4. 设$F\subseteq K\subseteq L$是一串扩域，其中F在K内是代数闭的。又设$\alpha\in L$是F上一个代数元。证明，$[K(\alpha):K]=[F(\alpha):F]$。

5. 设$F\subseteq E\subseteq K\subseteq L$是一串扩域，$F$在$K$内是代数闭的且$[K:E]<\infty$。又设$\alpha\in L$是$F$上一个代数元。证明，$[K(\alpha):E(\alpha)]=[K:E]$。

6. 设$K=\mathbf{Q}(\alpha)\subseteq \mathbf{C}$是$\mathbf{Q}$上一个单代数扩域且$\alpha\neq\bar{\alpha}$，$\bar{\alpha}\in K$（这里$\bar{\alpha}$表示$\alpha$的共轭复数）。证明：

（i）$[K:\mathbf{Q}]$是一个偶数，并且存在K在$\mathbf{Q}$上具有以下形状的一个基：

$$\gamma_1,\bar{\gamma}_1,\gamma_2,\bar{\gamma}_2,\cdots,\gamma_m,\bar{\gamma}_m.$$

(ii) 令$K_0=K\cap \mathbf{R}$。则$\gamma_1+\bar{\gamma}_1,\cdots,\gamma_m+\bar{\gamma}_m$是$K_0$在$\mathbf{Q}$上的一个基。

2.3 正规扩域　多项式的分裂域

在这一节里，我们将介绍一个域F上的一种很重要的代数扩域，称为正规扩域。正规扩域和F上一个多项式的分裂域有着密切的关系。我们将把这两个概念结合在一起来讨论。

先指出一个简单的事实。设F和F'都是域。如果存在F到F'的一个同态映射$\sigma:F\to F'$，那么σ可以用自然的方式开拓成为多项式环$F[X]$到$F'[X]$的同态映射。即对于

$$f(X)=a_0+a_1X+\cdots+a_nX^n\in F[X],$$

定义

$$\sigma(f(X))=\sigma(a_0)+\sigma(a_1)X+\cdots+\sigma(a_n)X^n\in F'[X]$$

以后我们对记号 $\sigma(f(X))$ 都作这样的理解。特别，当 σ 是 F 到 F' 的同构映射时，$\sigma: F[X] \to F'[X]$ 也是同构映射。

引理 2.3.1 设 K 是域 F 的一个代数扩域。那么 K 到 K 自身的每一个 F-同态单射都是满的，因而是 F-自同构。

证 设 $\sigma: K \to K$ 是一个同态单射，且保持 F 的元素不动。设 $\alpha \in K$。则 α 是 F 上代数元。令 $p(X)$ 是 α 在 F 上的最小多项式。设 $\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_m$ 是 $p(X)$ 在 K 内的一切互不相同的根。则在 $K[X]$ 内我们有

$$p(X) = (X - \alpha_1)^{k_1} \cdots (X - \alpha_m)^{k_m} g(X),$$

这里 $k_1, \cdots, k_m \geqslant 1$，$g(X) \in K[X]$ 且在 K 内没有根。对这个等式两端的系数作用 σ，因为 $p(X) \in F[X]$，所以 $\sigma(p(X)) = p(X)$。于是

$$p(X) = \sigma(p(X)) = (X - \sigma(\alpha_1))^{k_1} \cdots (X - \sigma(\alpha_m))^{k_m} \sigma(g(X))$$

$\sigma(g(X)) \in K[X]$。因为 σ 是单射，所以 $\sigma(\alpha_1), \cdots, \sigma(\alpha_m)$ 仍是 $p(X)$ 在 K 内一切互不相同的根。所以

$$\{\sigma(\alpha_1), \cdots, \sigma(\alpha_m)\} = \{\alpha_1, \cdots, \alpha_m\}.$$

这样一来，α 等于某个 $\sigma(\alpha_i)$，即 $\alpha \in \sigma(K)$。所以 σ 是满射。 ▌

现在引入一个概念。设 E 和 E' 都是域 F 的扩域。如果

（i） E 和 E' 都是 F 的某一扩域 L 的子域；

（ii） 存在一个 F-同构 $\varphi: E \to E'$。

那么就说，E 与 E' 在 F 上**共轭**，简称 **F-共轭**。在不致引起混淆的情况下，就称 E 与 E' **共轭**。如果 E 与 E' 共轭，那么就称 E 到 E' 的 F-同构映射为 **F-共轭映射**。

定义 设 F 是一个域。F 上一个扩域 E 叫做一个**正规扩域**，如果下列条件被满足：

（i） E 是 F 的代数扩域[1]；

---

1) 在正规扩域的定义中，条件(i)实际上是多余的，在第四章我们将证明，满足条件(ii)的扩域一定是代数的(参看4.1.1.3).

(ii) 任意与E在F上共轭的域都等于E。

如果E是F的一个正规扩域，那么也说E/F是一个正规扩张。

例 1 令$\mathbf{Q}$是有理数域，$E=\mathbf{Q}(\sqrt{2})$。则E是$\mathbf{Q}$的一个正规扩域。事实上，设σ是E的一个$\mathbf{Q}$-共轭。则$\sigma(\sqrt{2})$是$\sigma(X^2-2)=X^2-2$的一个根。然而X^2-2在E的任意一个扩域内只有两个根：$\sqrt{2}$和$-\sqrt{2}$，所以$\sigma(\sqrt{2})=\sqrt{2}$或$-\sqrt{2}$。不论哪一个情形都有$\sigma(E)=\mathbf{Q}(\sigma(\sqrt{2}))=\mathbf{Q}(\sqrt{2})=E$。

例 2 $E=\mathbf{Q}(\sqrt[3]{2})$不是$\mathbf{Q}$的正规扩域。因为在复数域$\mathbf{C}$内，$X^3-2$有三个根：$\sqrt[3]{2}$，$\zeta\sqrt[3]{2}$，$\zeta^2\sqrt[3]{2}$，这里
$\zeta=-\frac{1}{2}+\frac{1}{2}\sqrt{-3}$是一个三次单位根。显然$E'=\mathbf{Q}(\zeta\sqrt[3]{2})$是一个与$E$ $\mathbf{Q}$-共轭的域，但$E'\neq E$。

定理 2.3.2 设E是域F的一个代数扩域。对于E/F来说，下列三个条件是等价的：

(i) E/F是正规扩张；

(ii) 设Ω是F的任意一个包含E的代数闭包。那么对于Ω的任意一个F-自同构σ，都有$\sigma(E)=E$。

(iii) E的任意元素α在F上的最小多项式在$E[X]$中可以分解为一次因式的乘积。

证 (i)$\Longrightarrow$(ii) 设Ω是F的一个代数闭包且包含E。Ω的任意一个自同构σ将E映成一个与E是F-共轭的域$\sigma(E)$。因为E是F的正规扩域，所以$\sigma(E)=E$。

(ii)$\Longrightarrow$(iii) 设Ω是F的一个包含E的代数闭包。$\alpha\in E$在F上的最小多项式$p(X)$在$\Omega[X]$内分解成一次因式的积：

$$p(X)=(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n);$$

$\alpha_i\in\Omega$，$1\leqslant i\leqslant n$，且设$\alpha_1=\alpha$。由推论2.2.7，存在的Ω的F-自同构σ_i，使得$\sigma_i(\alpha)=\alpha_i$，$1\leqslant i\leqslant n$。因为$\alpha_i\in\sigma_i(E)=$

$E(1\leqslant i\leqslant n)$，所以$p(X)$在$E[X]$中可以分解成一次因式的积.

(iii)$\Longrightarrow$(i) 设E'是一个与E为F-共轭的域，由共轭的定义，E和E'都包含在F的某一扩域L内，并且存在F-同构映射$\psi: E\to E'$. 设$\alpha'\in E'$，令$\alpha=\psi^{-1}(\alpha')\in E$. 令$p(X)$是$\alpha$在$F$上最小多项式. 由(iii)，$p(X)$在$E[X]$内可以分解成一次因式的积：

$$p(X)=(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n),\ \alpha_i\in E(1\leqslant i\leqslant n).$$

因为$p(\alpha)=0$，所以$p(\alpha')=\psi(p(\alpha))=0$. 因此，在$L$内，等式

$$(\alpha'-\alpha_1)(\alpha'-\alpha_2)\cdots(\alpha'-\alpha_n)=0$$

成立. 于是α'必定等于某一个α_i，从而，$\alpha'\in E$. 因为α'是E'的任意元素，所以$E'\subseteq E$.

这样，$\psi: E\to E'\subseteq E$是E到自身内的一个同态单射. 因为E是F的代数扩域，由2.3.1，ψ是满射，从而$E'=\psi(E)=E$. 这就证明了E的任意一个F-共轭的域都与E相等，即E是F的正规扩域. ▌

推论 2.3.3 设E是域F的一个正规扩域. 对于E的元素α与β来说，以下两个条件是等价的：

(i) α与β在F上有同一个最小多项式；

(ii) 存在E的一个F-自同构σ，使得$\sigma(\alpha)=\beta$.

证 (i)$\Longrightarrow$(ii) 设Ω是E的一个代数闭包. Ω显然是F的一个包含E的代数闭包. 由2.2.7，存在Ω的一个F-自同构τ，使得$\tau(\alpha)=\beta$. E和$\tau(E)$都是Ω/F的中间域，且是F-共轭的. 由于E是正规的，所以$\tau(E)=E$. 这样，$\sigma=\tau|_E$是E的一个F-自同构，并且$\sigma(\alpha)=\beta$.

(ii)$\Longrightarrow$(i) 设$p(X)$是α在F上的最小多项式. 那么

$$p(\beta)=p(\sigma(\alpha))=\sigma(p(\alpha))=0.$$

所以$p(X)$也是β在F上的最小多项式. ▌

现在我们引入域F上一个多项式的分裂域的概念.

定义 设$f(X)$是域F上一个次数大于0的多项式。F的一个扩域K叫做$f(X)$在F上一个**分裂域**，如果

(i) $f(X)$在$K[X]$中可以分解成为一次因式的乘积：

$$f(X)=a(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n),$$
$$a\in F,\quad \alpha_i\in K(1\leqslant i\leqslant n);$$

(ii) $K=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$.

$F[X]$中任意一个次数大于0的多项式在F上总存在分裂域．事实上，取F上一个代数闭包Ω．则$f(X)$在$\Omega[X]$可以分解成为一次因式的积．将$f(X)$在Ω内的全部根添加到F上所得到的扩域K就是$f(X)$在F上的一个分裂域．

定理 2.3.4 设$f(X)$是域F上一个次数大于0的多项式，K和K'都是$f(X)$在F上的分裂域．在$K[X]$和$K'[X]$里，分别有

$$f(X)=a(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n),$$
$$f(X)=a(X-\alpha'_1)(X-\alpha'_2)\cdots(X-\alpha'_n),$$

$\alpha_i\in K,\alpha'_i\in K'(1\leqslant i\leqslant n)$，$a\in F$，那么存在$K$到$K'$的一个$F$-同构映射$\varphi$．使得

$$\{\varphi(\alpha_1),\cdots,\varphi(\alpha_n)\}=\{\alpha'_1,\cdots,\alpha'_n\}.$$

证 令Ω和Ω'分别是K和K'的代数闭包．它们也是F的代数闭包．由定理2.2.4，存在一个F-同构映射$\omega:\Omega\to\Omega'$．令$\alpha''_i=\omega(\alpha_i)$，$1\leqslant i\leqslant n$；$K''=F(\alpha''_1,\cdots,\alpha''_n)$．在$K''[X]$内，

$$f(X)=a(X-\alpha''_1)(X-\alpha''_2)\cdots(X-\alpha''_n).$$

因为$K''\subseteq\Omega'$，所以在$\Omega'[X]$内，$f(X)$有两种分解：

$$f(X)=a(X-\alpha'_1)(X-\alpha'_n)\cdots(X-\alpha'_n)$$
$$=a(X-\alpha''_1)(X-\alpha''_2)\cdots(X-\alpha''_n).$$

由域上多项式因式分解的唯一性，我们有

$$\{\omega(\alpha_1),\cdots,\omega(\alpha_n)\}=\{\alpha'_1,\cdots,\alpha'_n\},$$

从而$K''=K'$．令$\varphi=\omega|_K$就满足要求。 ∎

下面的定理表明正规扩域和多项式的分裂域这两个概念的密切联系。

定理 2.3.5 设K是域F的一个扩域。对于K来说，以下两个条件是等价的：

（i） K是F的有限次正规扩域；

（ii） K是$F[X]$的某一次数大于零的多项式在F上的分裂域。

证 (i)$\Longrightarrow$(ii) K是F的有限次扩域，由定理2.1.2，$K=F(\alpha_1,\cdots,\alpha_s)$，$\alpha_i$是$F$上代数元$(1\leqslant i\leqslant s)$。令$p_i(X)$是$\alpha_i$在$F$上的最小多项式。令

$$f(X)=\prod_{i=1}^{s}p_i(X).$$

由定理2.3.2(iii)，每一个$p_i(X)$在$K[X]$内可以分解成一次因式的乘积：

$$p_i(X)=\prod_{j=1}^{n_i}(X-\alpha_{ij}),\alpha_{ij}\in K,1\leqslant i\leqslant s.$$

于是在$K[X]$内，

$$f(X)=\prod_{i=1}^{s}\prod_{j=1}^{n_i}(X-\alpha_{ij}).$$

于是

$$K=F(\alpha_1,\cdots,\alpha_s)\subseteq F(\{\alpha_{ij}\});$$

$1\leqslant i\leqslant s,1\leqslant j\leqslant n_i$.

所以K是$f(X)$在F上的分裂域。

(ii)$\Longrightarrow$(i) 设K是$F[X]$中某一次数大于0的多项式$f(X)$在F上的分裂域。取K的一个代数闭包Ω，它也是F的代数闭包。在$\Omega[X]$中，

$$f(X)=a(X-\alpha_1)\cdots(X-\alpha_n),a\in F,\ \alpha_i\in\Omega.$$

那么$K=F(\alpha_1,\cdots,\alpha_n)$，由定理2.1.2，$[K:F]<\infty$。

设σ是Ω的任意一个F-自同构。σ自然地开拓为多项式环$\Omega[X]$的自同构，仍以σ表示。因为σ保持F的元素不动，我们有

$$f(X)=\sigma(f(X))=a(X-\sigma(\alpha_1))\cdots(X-\sigma(\alpha_n)).$$

由$\Omega[X]$中多项式因式分解的唯一性，我们有

$$\{\sigma(\alpha_1),\cdots,\sigma(\alpha_n)\}=\{\alpha_1,\cdots,\alpha_n\}.$$

所以$K=F(\alpha_1,\cdots,\alpha_n)=F(\sigma(\alpha_1),\cdots\sigma(\alpha_n))=\sigma(K)$。由2.3.2，$K$是$F$上的正规扩域。 ▮

由这个定理可以得出以下的推论。我们把这个推论的证明留给读者。

推论 2.3.6 设K是域F上的一个有限次扩域。对于K来说，以下两个条件是等价的：

(i) K是$F[X]$中某一个次数大于零的多项式在F上的分裂域；

(ii) $F[X]$内任意一个不可约多项式如果在K内有一个根，那么它在$K[X]$内可以分解成一次因式的乘积。 ▮

习 题

1. 证明，K/F是代数域扩张的充分且必要的条件是，对于K/F的每一个中间域E来说，如果$\sigma: E\to E$是F-同态单射，则σ必是E的F-自同构。

2. 试举一反例说明，当K不是域F的代数扩域时，定理2.3.1的结论不成立。

3. 下列域扩张哪些是正规扩张：

(i) $\boldsymbol{Q}(\sqrt{-3})/\boldsymbol{Q}$； (ii) $\boldsymbol{Q}(\sqrt[4]{2})/\boldsymbol{Q}$；

(iii) $\boldsymbol{C}/\boldsymbol{R}$； (iv) $\boldsymbol{C}/\boldsymbol{Q}$。

4. 证明，一个域F的二次扩域一定是F的正规扩域。

5. 设$F\subseteq K\subseteq L$是一串扩域，其中L/F是正规扩张。L/K是否正规？K/F是否正规？

如果L/K及K/F都是正规扩张，那么L/F是否正规？

6. 设$F[X]$是域F上一个不定元的多项式环，$\{f_\lambda\}_{\lambda\in\Lambda}$，其中$\Lambda$是一个指标集(有限或无限)，$\Omega$是$F$的一个代数闭包，令$K$是将$\{f_\lambda\}_{\lambda\in\Lambda}$在$\Omega$内的一切零点添加到$F$所得的扩域，证明，$K$是$F$的正规扩域。

7. 设K是域F的一个代数扩域，N是F的一个包含K的正规扩域。证明，K/F是正规扩张必要且只要K到N内的每一个F-同态单射都是K的自同构。

8. 设K是域F的一个代数扩域。证明，如果K的每一个元素都属于某一个中间域E，而E是F的正规扩域，则K是F的正规扩域。

9. 设Ω是域F的一个代数闭包，$N_\lambda\subseteq\Omega$(λ取遍某一个指标集Λ)都是F的正规扩域。令$N_1=\bigcap_{\lambda\in\Lambda}N_\lambda$，$N_2=F(\bigcup_{\lambda\in\Lambda}N_\lambda)$。证明，$N_1$，$N_2$都是$F$的正规扩域。

10. 设$f(X)$是域F上一个n($n>0$)次多项式，K是$f(X)$在F上一个分裂域。证明，$[K:F]\mid n!$。

11. 设K是域F的一个代数扩域。证明，对于K来说，以下两个条件是等价的：

(i) K是F的正规扩域；

(ii) $F[X]$中每一个不可约多项式$f(X)$在$K[X]$中若分解成为不可约因式的乘积，则所有这些不可约因式都有相同的次数。

12. 证明推论2.3.6。

2.4 有限域

只含有有限个元素的域叫做**有限域**。有限域的构造特别简单。在这一节里，我们将对于有限域作一比较全面的讨论。

设 F 是一个有限域。那么 F 所包含的素域 P 也是一个有限域。由1.2.1，这个素域所含的元素个数是一个素数 p。因此 $\text{char } F = p$。

设 F 含有 q 个元素，F 是素域 P 上有限次扩域。设 $[F:P]=f$，而 $\alpha_1, \cdots, \alpha_f$ 是 F 在 P 上一个基。，那么 F 的每一个元素 α 可以唯一地表示成

$$\alpha = a_1\alpha_1 + \cdots + a_f\alpha_f$$

的形式，$a_i \in P$，$1 \leqslant i \leqslant f$。因此 $q = p^f$。

令 $F^\times = F \setminus \{0\}$ 是 F 的一切非零元素所组成的集。则 $F^\times$ 是一个 $q-1$ 阶乘法群。$F^\times$ 的每一个元素都是方程 $X^{q-1}-1=0$ 的根。另一方面，$X^{q-1}-1=0$ 在 F 中至多有 $q-1$ 个根，所以

$$X^{q-1} - 1 = \prod_{\alpha \in F^\times}(X - \alpha).$$

这样，F 是多项式 $X^{q-1}-1$ 在素域 P 上的分裂域。同时 F 的每一个元素都是多项式

$$X^q - X = \prod_{\alpha \in F}(X - \alpha)$$

的根，所以 F 也是多项式 $X^q - X$ 在 P 上的的分裂域。

总结上面的讨论，我们得到

定理 2.4.1 设 F 是一个 q 元有限域，P 是 F 的素域。

(i) $\text{char } F = p > 0$；$q = p^f$；$[F:P] = f$。

(ii) $X^q - X = \prod_{\alpha \in F}(X - \alpha)$；$X^{q-1} - 1 = \prod_{\alpha \in F^\times}(X - \alpha)$。

(iii) F 是多项式 $X^q - X$ 和 $X^{q-1} - 1$ 在 P 上的分裂域. ∎

现在我们看两个有限域在什么时候是同构的。

定理 2.4.2 两个有限域是同构的当且仅当它们含有相同个数的元素。

证 设 F 和 F' 是两个有限域，它们分别含有 q 和 q' 个元素，如果 $F\cong F'$，那么自然有 $q=q'$。现在设 $q=q'$。令 $\mathrm{char}F=p$，$\mathrm{char}F'=p'$，由2.4.1，$q=p^f$，$q'=p'^{f'}$。则 $p^f=p'^{f'}$。因为 p 和 p' 都是素数，所以 $p=p'$，$f=f'$，因此，F 和 F' 各自所含的素域 P 和 P' 都是 p 元有限域，因而 $P\cong P'$。由2.4.1，F 和 F' 分别是多项式 X^q-X 在 P 和 P' 上的分裂域。由2.3.4，$F\cong F'$。 ▮

由于这个定理，我们通常把 q 元有限域记作 $\boldsymbol{F}_q$。

定理 2.4.3 设 K 是一个特征为素数 p 的域。$\boldsymbol{F}_q$ 和 $\boldsymbol{F}_{q'}$ 是 K 的两个有限子域，$q=p^f$，$q'=p^{f'}$。那么 $\boldsymbol{F}_q\subseteq\boldsymbol{F}_{q'}\Longleftrightarrow f|f'$。

证 K 的素域是 p 元有限域 $\boldsymbol{F}_p$。

如果 $\boldsymbol{F}_q\subseteq\boldsymbol{F}_{q'}$，那么

$$f'=[\boldsymbol{F}_{q'}:\boldsymbol{F}_p]=[\boldsymbol{F}_{q'}:\boldsymbol{F}_q][\boldsymbol{F}_q:\boldsymbol{F}_p]=mf,$$

这里 $m=[\boldsymbol{F}_{q'}:\boldsymbol{F}_q]$。

反之，设 $f'=mf$。$\boldsymbol{F}_q(\subseteq K)$ 是多项式 X^q-X 在 $\boldsymbol{F}_p$ 上的分裂域，所以

$$\boldsymbol{F}_q=\{\alpha\,|\,\alpha\in K,\ \alpha^q-\alpha=0\}.$$

同样，我们有

$$\boldsymbol{F}_{q'}=\{\beta\,|\,\beta\in K,\ \beta_{q'}-\beta=0\}.$$

于是

$$p^{f'}-1=(p^f)^m-1=(p^f-1)(p^{f(m-1)}+$$
$$+p^{f(m-2)}+\cdots+p^f+1).$$

如果 $\alpha\in\boldsymbol{F}_q^{\times}$，则

$$\alpha^{p^f-1}-1=\alpha^{q-1}-1=0.$$

于是

$$\alpha^{q^{f'}-1}-1=\alpha^{p^{f'}}-1=0.$$

所以 $\alpha\in F_{q^{f'}}^{\times}$。因此 $F_q^{\times}\subseteq F_{q^{f'}}^{\times}$，即 $F_q\subseteq F_{q^{f'}}$。 ∎

现在设给定了一个素数 p 和一个正整数 f。是不是存在一个 $q=p^f$ 个元素的有限域，下面的定理给予肯定的回答。

定理 2.4.4 设 p 是一个素数。

(i) 给了素域 F_p 的一个代数闭包 Ω。对于任意正整数 f，Ω 含有唯一的 $q=p^f$ 个元素的有限域，它是多项式 X^q-X 在 F_p 上的分裂域，

(ii) 对于 p 的任意幂 $q=p^f$，存在一个 q 元有限域，如果把同构的域看作一样的，那么这个有限域是唯一确定的。

证 显然(ii)是(i)和2.4.2的直接推论。因此我们只需证明(i)成立。

令 Ω 是 F_p 的一个代数闭包。令 $f(X)=X^q-X\in F_p[X]$。因为 $f'(X)=qX^{q-1}-1=-1\neq 0$，所以 $f(X)$ 在 Ω 内恰有 q 个两两不同的根。令

$$F=\{\alpha\mid\alpha\in\Omega,\alpha^q-\alpha=0\}.$$

则 F 含有 q 个元素。设 $\alpha,\beta\in F$。则

$$(\alpha-\beta)^q=\alpha^q-\beta^q=\alpha-\beta,$$

$$(\alpha\beta)^q=\alpha^q\beta^q=\alpha\beta.$$

如果 $\beta\neq 0$，则

$$(\beta^{-1})^q=(\beta^q)^{-1}=\beta^{-1}.$$

所以 F 是 Ω 的一个 q 元有限子域。它由 $f(X)$ 在 Ω 内的全部根组成，因而是 $f(X)$ 在 F_p 上的分裂域，所以是唯一确定的。 ∎

设 F_q 是一个有限域，$q=p^f$。令 e 是任意一个自然数。取定 F_q 的代数闭包 Ω。令

$$K=\{\alpha\mid\alpha\in\Omega,\alpha^{q^e}-\alpha=0\}.$$

则 K 是一个 $q^e=p^{ef}$ 个元素的有限域，并且含有 F_q 作为子域。

比较元素的个数，我们有

$$[K : F_q] = e.$$

于是就得到以下

定理 2.4.5 给定任意一个有限域 F_q 和任意正整数 e. 存在 F_q 的一个 e 次扩域. 它是一个 q^e 元有限域. F_q 的任意两个 e 次扩域是同构的. ∎

推论 2.4.6 设 F_q 是一个 q 元有限域. 令 Ω 是 F_q 的一个代数闭包. 则

$$\Omega = \bigcup_{f \geq 1} F_{q^f}.$$

证 令 Ω 是 F_q 的一个代数闭包. 对于任意正整数 f，由定理2.4.5的证明可以看出，在 Ω 内存在 F_q 的唯一的 f 次扩域 F_{q^f}. 所以 $\bigcup_{f \geq 1} F_{q^f} \subseteq \Omega$.

反之，设 $\alpha \in \Omega$，则 $F = F_q(\alpha)$ 是 F_q 的一个有限次扩域，因而 $F = F_{q^f}$，$f = [F : F_q]$. 所以 $\alpha \in F_{q^f} \subseteq \bigcup_{f \geq 1} F_{q^f}$. ∎

最后，我们证明，一个有限域的有限次扩域一定是单扩域. 为此我们要进一步弄清楚有限域的乘法群的结构. 先证明两个引理.

引理 2.4.7 设 G 是一个阶为 n 的有限群. 如果对于任意正整数 m 来说. G 中满足方程 $x^m = 1$ 的元素 x 的个数 $\leq m$，则 G 是一个循环群.

证 设 d 是 n 的任意一个正因数. 令 $\alpha_d(G)$ 表示 G 中阶为 d 的元素的个数. 那么

$$\sum_{\substack{1 \leq d \leq n \\ d \mid n}} \alpha_d(G) = n.$$

如果 $\alpha_d(G) \neq 0$，那么 G 中存在阶为 d 的元素 a. 令 H 是 a 所生成的环循子群. 则 H 含有 d 个元素，并且对于任意 $x \in H$，都满足 $x^d = 1$. 由题设的条件，我们有

$$H=\{x\in G \mid x^d=1\}.$$

因此，G中阶为d的元素都在H内．所以$\alpha_d(G)=\alpha_d(H)$．另一方面，H是阶为d的循环群，所以H所含的阶为d的元素等于$\varphi(d)$，这里φ是Euler函数，即$\varphi(d)$是小于d并且与d互素的正整数的个数．因此，对于n的任意正因数d来说，或者$\alpha_d(G)=0$，或者$\alpha_d(G)=\varphi(d)$．于是

$$n=\sum_{d\mid n}\alpha_d(G)\leqslant\sum_{d\mid n}\varphi(d)=n.$$

这样一来，对于n的任意正因数d来说，都有$\alpha_d(G)=\varphi(d)$．特别，$\alpha_n(G)=\varphi(n)\neq 0$．所以$G$含有阶为$n$的元素，从而$G$是循环群．

引理 2.4.8 设F是一个域，$F^\times$是F的一切非零元素所组成的乘法群．$F^\times$的任意有限子群都是循环群．

证 设G是$F^\times$的一个阶为n的子群．对于任意正整数来说，多项式X^m-1在F内至多有m个根，所以G中满足x^m-1的元素至多有m个．于是由2.4.7，G是循环群． ▮

由2.4.8，立即得到

定理 2.4.9 F_q的一切非零元素对于F_q的乘法来说作成一个$q-1$阶循环群． ▮

定理 2.4.10 有限域的有限次扩域都是单扩域．

证 设F_{q^f}是有限域F_q的一个f次扩域．令ζ是乘法群$F_{q^f}^\times$的个生成元．则

$$F_{q^f}^\times=\{1,\zeta,\cdots,\zeta^{q^f-2}\}.$$

所以．$F_{q^f}=F_q(\zeta)$． ▮

注意 在上面这个定理里，取ζ是乘法群$F_{q^f}^\times$的一个生成元，自然有$F_{q^f}=F_q(\zeta)$．然而反过来不一定对，也就是说，F_{q^f}可能是对F_q添加一个不是$F_{q^f}^\times$的生成元而得到的单扩域．

我们看以下的例子：

例 多项式

$$f(X)=X^4+X^3+X^2+X+1$$

在 $F_2[X]$ 内是不可约的。事实上，因为0和1都不是 $f(X)$ 的根，所以 $f(X)$ 在 $F_2[X]$ 内没有一次因式。很容易证明，在 $F_2[X]$，也不能分解成两个二次因式的乘积。

令 α 是 $f(X)$ 在 F_2 的某个扩域内的一个根。那么 $F_2(\alpha)=F_{2^4}$。然而 $\alpha^5-1=(\alpha-1)f(\alpha)=0$，所以 $\alpha^5=1$，因而 α 不是15阶循环群 $F_{2^4}^{\times}$ 的生成元。

习　题

1. 设 p 是一个素数。证明，对于任意整数 a 来说都有 $a^p\equiv a\pmod{p}$。

2. 设 p 是一个素数，$n>0$。证明 F_{p^n} 中每一个元素都在 F_{p^n} 中有唯一的 p 次根。

3. 设 K 是 q 元有限域 F_q 的一个代数扩域。证明 $\varphi: K\ni\alpha\longmapsto\alpha^q\in K$ 是 K 的一个自同构。

4. 构造一个有9个元素的域，并且给出它的加法及乘法表。

5. 证明，有限域不可能是代数闭域。

6. 设 F 是一个域，$f(X)$ 是 $F[X]$ 最高次项系数为1的多项式，它在 F 上某个分裂域中的根各不相同，并且构成一个域。证明 $\mathrm{char}F=p>0$，且 $f(X)=X^{p^n}-X$，其中 n 是一个正整数。

7. 设 F_q 是 q 元有限域，$(n,q)=1$，K 是多项式 X^n-1 在 F_q 上的分裂域。证明，$k=[K:F_q]$ 是使得 $n|q^k-1$ 的最小正整数。

8. 设 p 是一个素数。$q=p^f$。$f(X)\in F_q[X]$ 是一个 m 次不

可约多项式。

（i） 证明，$f(X)\mid(X^{q^n}-X)\Longleftrightarrow m\mid n$。

（ii） 令 $f_1(X),\cdots,f_s(X)$ 是 $F_q[X]$ 中一切最高次项系数是 1 且次数是 n 的因数的不可约多项式。证明

$$X^{q^n}-X=\prod_{i=1}^{s}f_i(X).$$

9. 找出 $F_2[X]$ 的一切四次不可约多项式。

10. 设 p 是一个素数。$a\in F_p$ 且 $a\neq 0$。证明，X^p-X+a 是 $F_p[X]$ 中不可约多项式。

11. 设 p 是一个素数。证明 $(p-1)!\equiv -1\pmod{p}$。

12. 构造一个满足下列条件的域 K：(i) K 是无限域；(ii) K 是一个有限域上的代数扩域；(iii) K 不是代数闭域。

13. 设 $q=p^f$。p 是一个素数，令 $F_q^{\times}$ 是 F_q 的一切非零元素所组成的乘法群。令

$$F_q^{\times 2}=\{\alpha^2\mid\alpha\in F_q^{\times}\}.$$

证明 $F_q^{\times 2}$ 是 $F_q^{\times}$ 的一个子群，并且 $(F_q^{\times}:F_q^{\times 2})=2$，若 $p\neq 2$；$(F_q^{\times}:F_q^{\times 2})=1$，若 $p=2$。

14. 设 F 是一个有限域。记

$$F^2+F^2=\{\alpha^2+\beta^2\mid\alpha,\beta\in F\}.$$

证明，$F^2+F^2=F$。

2.5 可分多项式和不可分多项式

一个域 F 的代数扩域中每一个元素都是 $F[X]$ 中一个不可约多项式的根。在这一节里，我们将对 $F[X]$ 的不可约多项式作一些讨论。

设 F 是一个域。$f(X)\in F[X]$ 是一个次数大于零的多项式。如果 $f(X)$ 在 F 的某一个代数闭包 Ω 内的根都是单根，那么就称

$f(X)$是一个**可分多项式**；如果 $f(X)$在Ω内有重根，就称 $f(X)$ 是一个**不可分多项式**。

这个定义不依赖于代数闭包的选取。事实上，设 Ω' 也是F的一个代数闭包。令$\{\alpha_1,\cdots,\alpha_n\}$和$\{\alpha'_1,\cdots,\alpha'_n\}$分别是$f(X)$在$\Omega$和$\Omega'$内的全部根。则 $K=F(\alpha_1,\cdots,\alpha_n)\subseteq\Omega$ 和 $K'=F(\alpha'_1,\cdots,\alpha'_n)\subseteq\Omega'$都是$f(X)$在$F$上的分裂域。于是存在$F$-同构$\sigma: K\to K'$，使得$\sigma(\alpha_i)=\alpha_i$。$\alpha_i\neq\alpha_j\Longleftrightarrow\alpha'_i\neq\alpha'_j$。不妨设$\alpha_1,\cdots,\alpha_r$是$f(X)$在$\Omega$内一切互不相同的根，那么$\alpha'_1,\cdots,\alpha'_r$就是$f(X)$在$\Omega'$内一切互不相同的根。因此，在$\Omega[X]$里，

$$f(X)=a(X-\alpha_1)^{k_1}\cdots(X-\alpha_r)^{k_r}$$

当且仅当在$\Omega'[X]$里，

$$f(X)=a(X-\alpha'_1)^{k_1}\cdots(X-\alpha_r)^{k_r}.$$

引理 2.5.1 设$f(X)$是域F上一个不可约多项式。$f(X)$是不可分的必要且只要$f'(X)=0$。

证 $f(X)$不可分$\Longleftrightarrow f(X)$与$f'(X)$不互素。又因为$f(X)$不可约。所以

$(f(X),f'(X))\neq 1\Longleftrightarrow f(X)\mid f'(X)\Longleftrightarrow f'(X)=0$. ▮

引理 2.5.2 设 $\mathrm{char}F=p>0$。$F[X]$的一个不可约多项式$f(X)$是不可分的必要且只要存在$h(X)\in F[X]$，使得

$$f(X)=h(X^p)$$

证 设$f(X)=\sum_{i=0}^{n}a_iX^i\in F[X]$是不可约的多项式。那么

$$f'(X)=\sum_{i=1}^{n}ia_iX^{i-1}.$$

如果 $f(X)$不可分。那么 $f'(X)=0$，而从$ia_i=0$ ($i=1,\cdots,n$)。因此，如果 $i\not\equiv 0 \bmod p$。则$a_i=0$，令

$$h(X)=a_0+a_pX+\cdots+a_{mp}X^m,$$

这里 $mp\leqslant n$，而$(m+1)p>n$。那么

$$f(X)=h(X^p).$$

反之，如果存在多项式 $h(X)\in F[X]$ 使得 $f(X)=h(X^p)$。那么 $f'(X)=pX^{p-1}\cdot h'(X^p)=0$，所以 $f(X)$ 不可分。 ∎

定理 2.5.3 设 $f(X)\in F[X]$ 是一个最高次项系数是 1 的 n 次不可约多项式。

（i） 如果 $\mathrm{char}F=0$，则 $f(X)$ 是可分的。

（ii） 如果 $\mathrm{char}F=p>0$，那么存在唯一的非负整数 e 和唯一的可分的不可约多项式 $g(X)\in F[X]$，使得 $f(X)=g(X^{p^e})$；并且 $p^e\deg(g(X))=n$。$f(X)$ 在 F 的一个代数闭包内恰有 m 个互不相同的根，每一个根的重数都是 p^e，这里 $m=\deg g(X)$。

证 设 $f(X)=\sum_{i=0}^{n}a_iX^i\in F[X]$，$a_n=1$。

（i） 如果 $f(X)$ 不可分，那么由引理2.5.1，$f'(X)=0$。从而 $ia_i=0\Longrightarrow a_i=0$，$i=1,\cdots,n$。于是 $f(X)=a_0\in F$，这与 $f(X)$ 的不可约性矛盾。

（ii） 考虑这样的 $u(X)\in F[X]$：存在一个非负整数 s，使得 $u(X^{p^s})=f(X)$。令 S 是一切满足上述条件的非负整数所成的集。$S\neq\varnothing$，因为 $0\in S$。对于任意 $s\in S$，设 $u(X^{p^s})=f(X)$。那么

$$n=p^s\cdot\deg(u(X))\geqslant p^s.$$

所以

$$s\leqslant\frac{\log n}{\log p}.$$

因此 S 有上界，从而是一个有限集。令 e 是 S 中最大的数。那么存在 $g(X)\in F[X]$，使得

$$g(X)=g(X^{p^e}),$$

并且对于任意非负整数 $f>e$，不存在 $v(X)\in F[X]$，使得 $f(X)$

$=v(X^{p^s})$. 显然，$g(X)$的最高次项系数是 1 . 我们证明，$g(X)$是$F[X]$中可分的不可约多项式. 如果

$$g(X)=g_1(X)g_2(X),$$

$g_i(X)\in F[X](i=1, 2)$，则

$$f(X)=g(X^{p^e})=g_1(X^{p^e})g_2(X^{p^e}).$$

因为$f(X)$不可约，所以$g_1(X^{p^e})$与$g_2(X^{p^e})$中必有一个是零次多项式，从而$g_1(X)$与$g_2(X)$中必有一个是零次多项式，所以$g(X)$不可约.

因为$f(X)$不再能表示成F上的$X^{p^{e+1}}$的多项式，所以不存在$h(X)\in F[X]$使得$g(X)=h(X^p)$. 由2. 5. 2，$g(X)$是可分的.

设 $m=\deg(g(X))$. 则$n=p^e m$. 令 Ω 是F的一个代数闭包. 在$\Omega[X]$内，可分多项式$g(X)$分解成m个两两互素的一次因式的乘积：

$$g(X)=(X-\beta_1)(X-\beta_2)\cdots(X-\beta_m).$$

$\beta_i\in\Omega(1\leqslant i\leqslant m)$. 对于每一个$i$，令$\alpha_i$是多项式$X^{p^e}-\beta_i$在$\Omega$内的一个根. 那么在$\Omega[X]$内，

$$X^{p^e}-\beta_i=X^{p^e}-\alpha_i^{p^e}=(X-\alpha_i)^{p^e},$$

并且$\alpha_i\neq\alpha_j$，若$i\neq j$. 于是在$\Omega[X]$内，

$$\begin{aligned}f(X)=g(X^{p^e})&=(X^{p^e}-\beta_1)\cdots(X^{p^e}-\beta_m)\\&=(X-\alpha_1)^{p^e}\cdots(X-\alpha_m)^{p^e}.\end{aligned}$$

所以$f(X)$在Ω中恰有m个两两不同的p^e重根$\alpha_1, \alpha_2, \cdots, \alpha_m$. 这个事实显然不依赖于代数闭包$\Omega$的选取.

最后只剩下证明，$g(X)$和e都由$f(X)$唯一确定. 如果有可分的不可约多项式$g_1(X)$，$g_2(X)$和非负整数e_1，e_2使得，

$$f(X)=g_1(X^{p^{e_1}})=g_2(X^{p^{e_2}})$$

令$m_i=\deg(g_i(X))$，$i=1. 2$，而Ω是F的一个代数闭包，那么由以上的证明，在$\Omega[X]$内有

$$f(X)=g_1(X^{p^{e_1}})=(X-\alpha_1)^{p^{e_1}}\cdots(X-\alpha_{m_1})^{p^{e_1}}.$$

$$=(X-\alpha'_1)^{p^{e_2}}\cdots(X-\alpha'_{m_2})^{p^{e_2}},$$

$\alpha_1,\cdots,\alpha_{m_1}\in\Omega$两两不同，$\alpha'_1,\cdots,\alpha'_{m_2}\in\Omega$两两不同。由因式分解的唯一性得出$m_1=m_2$，$p^{e_1}=p^{e_2}$，从而$e_1=e_2$，并且适当对$\alpha'_1,\cdots,\alpha'_{m_2}$编号，可以使$\alpha_i=\alpha'_i$，$1\leqslant i\leqslant m_1=m_2$，从而$g_1(X)=g_2(X)$。 ▮

推论 2.5.4 在定理2.5.3的记号和假设下，$f(X)$可分当且仅当$e=0$。 ▮

由2.5.3，当$\mathrm{char}F=p>0$时，对于$F[X]$中每一个不可约多项式$f(X)$，有唯一的可分的不可约多项式$g(X)$和非负整数e，使得$f(X)=g(X^{p^e})$。这个多项式$g(X)$的次数叫做$f(X)$的**约化次数**，e叫做$f(X)$的**不可分指数**，p^e叫做$f(X)$的**不可分次数**。我们有

$$\deg(f(X))=（不可分次数）\times（约化次数）.$$

当$\mathrm{char}F=0$时，任何不可约多项式都是可分的，这时可以认为不可分指数是0而不可分次数是1，并且约化次数等于$\deg(f(X))$。

由2.5.3我们还看到，当$\mathrm{char}F=p>0$时．$F[X]$中不可约多项式$f(X)$在它的分裂域内一切互不相同的根的个数等于$f(X)$的约化次数，如果$f(X)$在它的分裂域中的根完全相同，即$f(X)$的约化次数等于1，这时称$f(X)$是**纯不可分的**。

纯不可分的多项式都具有$X^{p^e}-a(a\in F)$的形状。

习　题

1. 设$f(X)$是域F上一个n次不可约多项式，且$\mathrm{char}F\nmid n$。证明$f(X)$在F上是可分的。

2. 设$f(X)$是域F上一个最高次项系数为1的不可约多项式，$\deg f(X)\geqslant 2$。如果$f(X)$在它的一个分裂域内所有的根都相同，则$\mathrm{char}F=p>0$，且$f(X)=X^{p^n}-a\in F$，$n\geqslant 1$。

3. 设F是一个特征为$p>0$的域。$a\in F$但$a\notin F^p=\{b^p|b\in F\}$。证明，对于每一个$n>1$，$X^{p^n}-a$是$F$上不可约多项式。

4. 设F是一个特征为$p>0$的域，$f(X)=\sum_{i=0}^{n}a_iX^i$是$F$上一个可分多项式。证明，$g(X)=\sum_{i=0}^{n}a_i^pX^i$也是$F$上可分多项式。

5. 设F_p是p个元素的素域，t是F_p上一个不定元，$F=F_p(t)$。证明，多项式X^p-t是F上一个纯不可分的不可约多项式。

6. 设F是一个特征为$p>0$的域，α是F的一个扩域K中的元素，$\alpha^{p^e}=a\in F$但$\alpha^{p^{e-1}}\notin F$。证明，$X^{p^e}-a$在F上不可约。

7. 设k是一个特征为$p>0$的域，$F=k(t_1,t_2)$，t_1,t_2是k上不相关不定元。证明，$f(X)=X^{2p}+t_1X^p+t_2$在F上不可约。求$f(X)$的约化次数和不可分指数。

2.6 共轭映射的个数

设F是一个域，Ω是F的一个代数闭包。K是扩张Ω/F的一个中间域。K到Ω内的一个F-同态单射叫做K到Ω内的一个**F-共轭映射**，简称为**F-共轭**。设$\sigma: K\to\Omega$是一个F-共轭。那么$\sigma(K)$也是Ω/F的一个中间域，并且$\sigma(K)$与K是F-共轭的。

令A是K到Ω内的一切F-共轭所成的集。我们把A的基数（K的F-共轭的个数）记作$\iota(K/F,\Omega)$。

$\iota(K/F,\Omega)$不依赖于代数闭包Ω的选取。事实上，设Ω和Ω'都是F的代数闭包并且都包含K。那么存在F-同构映射$\omega: \Omega\to\Omega'$。令A和A'分别是K到Ω内的F-共轭和K到Ω'内的F-共轭所成的集。对于任意$\sigma\in A$，则$\omega\circ\sigma\in A'$。反过来，对于任意$\sigma'\in A'$，则$\omega^{-1}\circ\sigma'\in A$。因此，

$$A\in\sigma\longmapsto\sigma'=\omega\circ\sigma\in A'$$

是A到A'的双射，从而$\iota(K/F, \Omega)=\iota(K/F, \Omega')$。因此，对于代数扩张$K/F$来说，我们任意取定$F$的一个包含$K$的代数闭包$\Omega$，而把$K$到$\Omega$内的$F$-共轭的个数记作$\iota(K/F)$。

定理 2.6.1 设K是代数扩张L/F的一个中间域。那么

$$\iota(L/F)=\iota(L/K)\iota(K/F).$$

证 令Ω是L的一个代数闭包。因为L/F是代数扩张，Ω自然也是K和F的代数闭包。令$\{\lambda_i\}_{i\in I}$是K到Ω内的F-共轭的全体；$\{\mu_j\}_{j\in J}$是L到Ω内的K-共轭的全体。对于任意$i\in I$和$j\in J$，由推论2.2.6，λ_i可以开拓为Ω的一个F-自同构λ'_i；μ_j可以开拓为Ω的一个F-自同构μ'_j。于是$\mu'_i\circ\mu'_j$是Ω的一个F-自同构。对于$(i,j)\in I\times J$，令φ_{ij}表示$\lambda'_i\circ\mu'_j$在L上的限制。那么φ_{ij}是L到Ω内的一个F-共轭。因此，我们只需证明以下两点：

1° $(i,j)\neq(k,l)\Longrightarrow\varphi_{ij}\neq\varphi_{kl}$；

2° 设$\varphi: L\to\Omega$是L到Ω内的一个F-共轭。那么存在$(i,j)\in I\times J$，使得$\varphi_{ij}=\varphi$。

先证1°。如果$\varphi_{ij}=\varphi_{kl}$。那么对于任意$\alpha\in K\subseteq L$，都有$\varphi_{ij}(\alpha)=\varphi_{kl}(\alpha)$。由于$\alpha\in K$，所以

$$\varphi_{ij}(\alpha)=\lambda'_i(\mu'_j(\alpha))=\lambda'_i(\alpha)=\lambda_i(\alpha).$$

$$\varphi_{kl}(\alpha)=\lambda'_k(\mu'_l(\alpha))=\lambda'_k(\alpha)=\lambda_k(\alpha).$$

因此$\lambda_i(\alpha)=\lambda_k(\alpha)$。这样就有$\lambda_i=\lambda_k$，从而$i=k$。

设$\beta\in L$。我们有

$$\lambda'_i(\mu_j(\beta))=\lambda'_i\mu'_i((\beta))==\varphi_{ij}(\beta)$$

$$=\varphi_{kl}(\beta)=\lambda'_k(\mu'_l(\beta))=\lambda'_k(\mu_l(\beta)).$$

我们已经证明了，$i=k$，又因为λ'_i是单射，所以$\mu_j(\beta)=\mu_l(\beta)$，因此$\mu_j=\mu_l$，从而$j=l$，这就证明了

$$\varphi_{ij}=\varphi_{kl}\Longrightarrow(i,j)=(k,l).$$

再证2°成立。设$\varphi: L\to\Omega$是L到Ω内一个F-共轭。令$\bar{\varphi}=\varphi|_K$。则$\bar{\varphi}$是K到Ω内一个F-共轭。于是有$i\in I$，使得

$\tilde{\varphi}=\lambda_i$，对于任意$\alpha\in K$来说，

$$\varphi(\alpha)=\tilde{\varphi}(\alpha)=\lambda_i(\alpha)=\lambda'_i(\alpha).$$

所以$\lambda'^{-1}_i(\varphi(\alpha))=\alpha$，即$\lambda'^{-1}_i\circ\varphi$是$L$到$\Omega$内一个$F$-共轭.于是有$j\in J$，使得$\lambda'^{-1}_i\circ\varphi=\mu_j$。这样，$\varphi=\lambda'_i\circ\mu_j$是$\lambda'_i\circ\mu'_j$在$L$上的限制$\varphi_{ij}$。定理被证明。 ▌

定理 2.6.2 设$K=F(\alpha)$是域F的一个单代数扩域，$p(X)$是α在F上的最小多项式。那么

$$\iota(K/F)=p(X)\text{的约化次数}.$$

证 令Ω是K的一个代数闭包。设m是$p(X)$的约化次数。那么$p(X)$在Ω内有m个互不相同的根$\alpha_1,\cdots,\alpha_m$，其中$\alpha=\alpha_1$。由2.2.7，存在Ω的F-自同构ω_i使得$\omega_i(\alpha)=\alpha_i$，$1\leqslant i\leqslant m$。令$\varphi_i$是$\omega_i$在$K$上的限制。则$\varphi_i$是$K$到$\Omega$内的$F$-共轭。当$i\neq j$时，$\varphi_i(\alpha)=\alpha_i\neq\alpha_j=\varphi_j(\alpha)$，所以$\varphi_i\neq\varphi_j$。这样，$\varphi_1,\cdots,\varphi_m$是$K$到$\Omega$内的互不相同的$F$-共轭，所以$m\leqslant\iota(K/F)$。

设φ是K到Ω内的一个F-共轭。令$\alpha'=\varphi(\alpha)\in\Omega$。则$p(\alpha')=p(\varphi(\alpha))=\varphi(p(\alpha))=0$.所以$\alpha'$等于某一个$\alpha_i=\varphi_i(\alpha)$，$1\leqslant i\leqslant m$。对于这个$i$，令

$$K'=\{\beta\mid\beta\in K;\ \varphi(\beta)=\varphi_i(\beta)\}.$$

易证K'是K的一个子域且$K'\supseteq F$,$K'\ni\alpha$.所以$K'\supseteq F(\alpha)=K$，从而$K'=K$。因此$\varphi=\varphi_i$。这就证明了$\iota(K/F)\leqslant m$。 ▌

注意到一个不可约多项式$p(X)$是可分的当且仅当它的约化次数等于$p(X)$的次数，我们立即得到以下

推论 2.6.4 记号同2.6.2。那么

$$p(X)\text{可分}\Longleftrightarrow\iota(K/F)=[K:F].$$ ▌

定理2.6.4 设K是域F的一个有限次扩域。那么

$$\iota(K/F)\leqslant[K:F].$$

证 因为$[K:F]<\infty$，所以K是由F上有限个代数元生成的域。设

$$K=F(\alpha_1,\cdots,\alpha_n),\ \ \alpha_i\in K,\ \ 1\leqslant i\leqslant n.$$

令$F_0=F$，$F_i=F_{i-1}(\alpha_i)=F(\alpha_1,\cdots,\alpha_i)$，$1\leqslant i\leqslant n$，我们得到一个扩域序列

$$F=F_0\subseteq F_1\subseteq\cdots\subseteq F_n=K.$$

每一个 F_i是前一个域 F_{i-1} 的单代数扩域。于是由2.6.1和2.6.2，我们有

$$\iota(K/F)=\prod_{i=1}^{n}\iota(F_i/F_{i-1})\leqslant\prod_{i=1}^{n}[F_i:F_{i-1}]=[K:F].\quad ▮$$

习　题

1. 令$\overline{Q}$表示有理数域Q在C内的代数闭包（即一切代数数所成的数域）．找出域K到$\overline{Q}$内的所有Q-同构，其中

(i)　$K=\overline{Q}(\sqrt[3]{2})$；(ii)　$K=\overline{Q}(e^{2\pi i/5})$。

2.7　可分扩域和不可分扩域

设K是域F的一个扩域，$\alpha\in K$是F上一个代数元。如果α在F上的最小多项式是可分的，那么就称α是F上一个**可分元素**。类似地，如果α在F上的最小多项式是不可分或者是纯不可分的，那么相应地就称α是F上**不可分**或**纯不可分元素**。

根据这个定个定义，特征为零的域上每一个代数元都是可分的。我们看一看，当域F的特征是一个素数p时，F上的元素在什么时候可分。

定理 2.7.1　设F是一个特征为$p>0$的域，K是F的一个扩域，$\alpha\in K$是F上一个代数元。令e是α在F上最小多项式的不可分指数。则α^{p^e}是F上可分元素。

证　设$p(X)$是α在F上的最小多项式。由定理2.5.3，存在一个可分的不可约多项式$g(X)\in F[X]$，使得$p(X)=g(X^{p^e})$，$g(\alpha^{p^e})=f(\alpha)=0$。所以$g(X)$是$\alpha^{p^e}$在$F$上的最小多项式，因

而α^{p^e}是F上可分元素。 ∎

定理 2.7.2 设E是域扩张K/F的一个中间域，$\alpha\in K$是F上的代数元。如果α在F上可分，那么α也在E上可分。

证 令α在F上和E上的最小多项式分别是$f(X)$和$g(X)$。在$E[X]$内，$g(X)|f(X)$。因为$f(X)$没有重根，所以$g(X)$也没有重根，从而$g(X)$是E上可分多项式，α是E上可分元素。 ∎

定理 2.7.3 设K是特征为$p>0$的域F上一个扩域，$\alpha\in K$是F上一个代数元。α在F上可分必要且只要对于任意非负整数n，都有

$$F(\alpha)=F(\alpha^{p^n}).$$

证 设α在F上可分。令$f(X)$是α在$F(\alpha^p)$上的最小多项式。由2.7.2，$f(X)$是$F(\alpha^p)$上可分多项式，所以没有重根。另一方面，α是$F(\alpha^p)$上多项式$X^p-\alpha^p$的根。所以在$F(\alpha^p)[X]$内，$f(X)$整除$X^p-\alpha^p$。这样，必须$f(X)=X-\alpha$，从而$\alpha\in F(\alpha^p)$。于是就得到

$$F(\alpha)=F(\alpha^p)=F[\alpha^p].$$

因此α可以表成α^p的系数属于F的多项式：

$$\alpha=\sum_{k=0}^{m}a_k\alpha^{kp},\ a_k\in F.$$

两边举p次方得

$$\alpha^p=\sum_{k=0}^{m}a_k^p\alpha^{kp^2}\in F[\alpha^{p^2}]=F(\alpha^{p^2}).$$

所以$F(\alpha^p)=F(\alpha^{p^2})$。同样的推理，我们有

$$F(\alpha)=F(\alpha^p)=F(\alpha^{p^2})=\cdots=F(\alpha^{p^n})=\cdots$$

现在设α在F上不可分。令$p(X)$是α在F上最小多项式。那么存在$g(X)\in F[X]$，使得$p(X)=g(X^p)$。所以$g(\alpha^p)=0$。于是

$$[F(\alpha^p):F]\leqslant\deg(g(X))<\deg(p(X))=[F(\alpha):F].$$

因而$F(\alpha^p)\subsetneqq F(\alpha)$. ▌

定理 2.7.4 设K是特征为$p>0$的域F的一个代数扩域，Ω是K的一代数闭包. 对于K的元素α来说，下列三个条件是等价的：

(i) α是F上的纯不可分元素；

(ii) 存在一个整数$e\geqslant 0$，使得$\alpha^{p^e}\in F$；

(iii) 对于K到Ω内的任意一个F-共轭φ来说，都有$\varphi(\alpha)=\alpha$.

证 (i)$\Longrightarrow$(ii) α在F上是纯不可分的，所以α在F上最小多项式有形状$X^{p^e}-a$，$a\in F$，$e\geqslant 0$. 从而$\alpha^{p^e}=a\in F$.

(ii)$\Longrightarrow$(iii) 设存在整数$e\geqslant 0$使得$\alpha^{p^e}=a\in F$，令φ是K到Ω内的一个F-共轭映射. 则$\varphi(\alpha^{p^e})=\varphi(a)=a=\alpha^{p^e}$. 于是

$$(\varphi(\alpha)-\alpha)^{p^e}=\varphi(\alpha^{p^e})-\alpha^{p^e}=0.$$

所以$\varphi(\alpha)=\alpha$.

(iii)$\Longrightarrow$(i) 由2.2.6，$F(\alpha)(\subseteq K)$到Ω内的任意一个F-共轭φ可以开拓为Ω的一个F-自同构$\tilde{\varphi}$. $\tilde{\varphi}|_K$是K到Ω内的一个F-共轭. 因为$\alpha\in K$，所以$\varphi(\alpha)=\widetilde{\varphi}(\alpha)=\alpha$. 所以$\varphi$是$F(\alpha)$到自身的恒等自同构，因而$\iota(F(\alpha)/F)=1$. 由2.6.2，$\alpha$在$F$上的最小多项式$p(X)$的约化次数等于1，从而$p(X)$是$F$上一个纯不可分多项式，$\alpha$是$F$上一个纯不可分元素. ▌

现在我们引入可分扩域和不可分扩域的概念.

设K是域F的一个代数扩域. 如果K的每一个元素都是F上可分元素，那么就称K是F的一个**可分扩域**. 在相反的情形，即K中至少存在F上一个不可分元素，就称K是F上一个**不可分扩域**.

当$\mathrm{char}F=0$时，F的任何代数扩域都是F上可分扩域. 当$\mathrm{char}F=p>0$时，也存在F上可分扩域，因为我们有

定理 2.7.5 有限域的代数扩域是可分的.

证 设F是一个有限域，K是F的一个代数扩域．设$\alpha\in K$，则$F(\alpha)$是F的一个有限次扩域，因而也是一个有限域，设$F(\alpha)=F_q$．那么α是可分多项式$X^q-X\in F[X]$的根．因此，作为X^q-X的一个因式，α在F上的最小多项式也是可分的．从而α是F上可分元素． ∎

让我们看一个不可分扩域的例子．

例 设k是一个特征为$p>0$的域，t是k上一个不定元．令$F=k(t)$．设n是一个正整数且$p|n$，多项式$f(X)=X^n-t\in F[X]$是不可约的．实事上，t是环$k[t]$的一个不可约元素，由Eisenstein判断法，$f(X)$不能分解成为系数在$k[t]$内的两个次数都低于n的多项式的积．因而在$k[t]$的商域$F=k(t)$上不可约．又因为$f'(X)=nX^{n-1}=0$，所以$f(X)$是F上不可分的多项式．令Ω是F的一个代数闭包，$\alpha\in\Omega$是$f(X)$的一个根．由于α在F上最小多项式$f(X)$不可分，所以$\alpha=t^{1/n}$是F上不可分元素，因而$K=F(\alpha)$是F的一个n次不可分扩域．

定理 2.7.6 设K是域F的一个扩域．对于K来说，下列三个条件是等价的：

（i） K是F的有限次可分扩域；

（ii） $K=F(\alpha_1,\cdots,\alpha_n)$，每一个$\alpha_i\in K$都是$F$上可分元素，$i=1,\cdots,n$；

（iii） $\iota(K/F)=[K:F]<\infty$．

证 (i)$\Longrightarrow$(ii) K是F的有限次扩域，于是由2.1.2，$K=F(\alpha_1,\cdots,\alpha_n)$，每一个都是$F$上代数元．又因为$K$是$F$上可分扩域，所以每一个$\alpha_i(1\leqslant i\leqslant n)$都是$F$上可分元素．

(ii)$\Longrightarrow$(iii) $K=F(\alpha_1,\cdots,\alpha_n)$，每一个$\alpha_i$都是$F$上可分元素．仍由2.1.2，$[K:F]<\infty$．令$F_0=F$，$F_i=F(\alpha_1,\cdots,\alpha_i)$，$i=1,\cdots,n$，我们有以下的扩域序列：

$$F=F_0\subseteq F_1\subseteq\cdots\subseteq F_n=K,\quad F_i=F_{i-1}(\alpha_i),\ 1\leqslant i\leqslant n.$$

由2.7.2，每一个α_i都是F_{i-1}上的可分元素。再由2.6.3，

$$\iota(F_i/F_{i-1})=[F_i:F_{i-1}],\ 1\leqslant i\leqslant n.$$

于是由2.6.1，

$$\iota(K/F)=\prod_{i=1}^{n}\iota(F_i/F_{i-1})=\prod_{i=1}^{n}[F_i:F_{i-1}]=[K:F].$$

(iii)$\Longrightarrow$(i) 我们只需证明，K的每一个元素都是F上可分元素。设$\alpha\in K$。由2.6.4，

$$\iota(F(\alpha)/F)\leqslant[F(\alpha):F],\iota(K/F(\alpha))\leqslant[K:F(\alpha)].$$

这样一来就有

$$[K:F]=\iota(K/F)=\iota(K/F(\alpha))\iota(F(\alpha)/F)$$
$$\leqslant[K:F(\alpha)][F(\alpha):F]=[K:F].$$

因此必须$\iota(F(\alpha)/F)=[F(\alpha):F]$（同时也有$\iota(K/F(\alpha))=[K:F(\alpha)]$）。由2.6.3，$\alpha$是$F$上可分元素。 ▮

推论 2.7.7 设$K=F(S)$，$S\subseteq K$是由域F上一些可分元素所组成的集。则K是F的可分扩域。

证 由2.1.3，可以归结为是有限集的情形，而后一情形正是定理2.7.6。 ▮

定理 2.7.8 设K是域F的一个代数扩域，E是扩张K/F的一个中间域。

$$K/F\text{可分}\Longleftrightarrow K/E\text{和}E/F\text{都可分。}$$

证 设K/F可分，由2.7.2推出K/E可分；又$E\subseteq K$，所以E/F自然可分。

反之，设$\alpha\in K$。令

$$g(X)=X^m+\beta_1X^{m-1}+\cdots+\beta_m,\beta_i\in E.$$

是α在E上的最小多项式。那么$g(X)$是E上可分多项式。又根据假设和2.7.6，$E'=F(\beta_1,\cdots,\beta_m)\subseteq E$是$F$的有限次可分扩域，所以

$$\iota(E'/F)=[E':F]<\infty.$$

另一方面，$g(X)$是$E'[X]$的一个不可约多项式，所以$g(X)$也是α在E'上的最小多项式。于是由2.6.3，

$$\iota(E'(\alpha)/E')=[E'(\alpha):E'].$$

于是就有

$$\iota(E'(\alpha)/F)=\iota(E'(\alpha)/E')\iota(E'/F)=[E'(\alpha):E'][E':F]$$
$$=[E'(\alpha):F]<\infty.$$

所以$E'(\alpha)=F(\beta_1,\cdots,\beta_m,\alpha)$是$F$的一个有限次可分扩域，从而$\alpha$是$F$上可分元素。这就证明了$K/F$是可分扩张。 ▮

定理 2.7.9 设K是域F的一个代数扩域。令S是K中在F上可分元素的全体。则$F\subseteq S$，并且S是K的一个在F上可分的子域。

证 对于F的任意元素a，a在F上的最小多项式$X-a$自然是F上可分多项式，所以$F\subseteq S$。

设$\alpha,\beta\in S$。由2.7.6，$F(\alpha,\beta)$是F的可分扩域，所以$\alpha-\beta$，$\alpha\beta$都是F上可分元素，从而属于S；如果$\beta\neq 0$，则$\beta^{-1}\in S$，所以S是K的一个子域。S自然是F的可分扩域。 ▮

设K是域F的一个代数扩域。由K中一切在F上可分元素所组成的子域S叫做F在K内的**可分闭包**。S显然是K的一切在F上可分的子域中最大者。

域F在F的一个代数闭包内的可分闭包简称作F的可分闭包.

显然，域F的一个代数扩域K是可分的充要条件是F在K内的可分闭包与K重合。

习　题

1. 设F是一个特征为$p>0$的域，K是F的一个有限次扩域且$p\nmid[K:F]$。证明，K是F的可分扩域。

2. 设F是一个特征为$p>0$的域，$K=F(\alpha,\beta)$，这里α是F上n次可分元素而β是F上p次不可分元素。求$[K:F]$。

3. 设F是一个特征为$p>0$的域. 多项式$f(X)\in F[X]$叫做一个**p-多项式**, 如果$f(X)$具有形状$X^{p^m}+a_1X^{p^{m-1}}+\cdots+a_mX$. 证明, 一个$p$-多项式的根组成其分裂域的加法群的一个有限子群,且每一个根都有相同的重数p^e, e是一个非负整数.

4. 设F是一个特征为$p>0$的域, $a\in F$. 证明:

(i) $f(X)=X^p-X-a$没有重根;

(ii) $f(X)$在$F[X]$中不可约必要且只要对于任何$c\in F$来说, $a\neq c^p-c$.

5. 设K是域F的一个扩域, $\alpha,\beta\in K$, 其中α是F上一个可分元素而β是F上一个纯不可分元素. 证明, $F(\alpha,\beta)=F(\alpha+\beta)$. 如果$\alpha\beta\neq 0$, 则$F(\alpha,\beta)=F(\alpha+\beta)=F(\alpha\beta)$.

6. 设K是域F的一个代数扩域, K_i是K中一切在F上纯不可分的元素所成的集. 证明, K_i是K/F的一个中间域.

7. 设K,L都是域扩张M/F的中间域, 证明:

(i) 如果K/F是可分扩张, 则KL/L是可分扩张;

(ii) 如果K/F, L/F都是可分扩张, 则KL/F也是可分扩张.

8. 设K是域F的一个可分扩域, Ω是K的一个代数闭包. 证明, 对于K的元素α来说, 以下两条件是等价的:

(i) $\alpha\in F$; (ii) 对于K到Ω内的任意F-同构σ来说, 都有$\sigma(\alpha)=\alpha$.

9. 设K是域F的一个代数扩域, $\operatorname{char}F=p>0$. 证明:

(i) 如果K是F上可分扩域, 则对于任意正整数e来说, 都有$K=FK^{p^e}$;

(ii) 如果$[K:F]<\infty$, 且$K=FK^p$, 则K是F上可分扩域.

2.8 纯不可分扩域 可分次数和不可分次数

设K是域F的一个代数扩域．如果F在K内的可分闭包与F重合，那么就称K是F的一个**纯不可分扩域**．相应地，称K/F是一个**纯不可分扩张**．这个条件相当于说，$K\setminus F$的每一个元素都是F上的不可分元素．

定理 2.8.1 设K是域F的一个代数扩域，S是F在K内的可分闭包．那么K是S上纯不可分扩域．

证 令S'是S在K内的可分闭包，则S'是S的一个可分扩域．又S是F的可分扩域，所以S'是F的可分扩域，从而$S'\subseteq S$．这样，$S'=S$，即K是S的纯不可分扩域． ▮

根据纯不可分域扩张的定义，与定理2.7.4完全平行，我们有

定理 2.8.2 设F是一个特征为$p>0$的域．对于F的一个代数扩域K来说，下列三个条件是等价的：

(i) K是F的纯不可分扩域；

(ii) 对于任意$\alpha\in K$，存在整数$e\geqslant 0$，使得$\alpha^{p^e}\in F$；

(iii) $\iota(K/F)=1$． ▮

推论 2.8.3 设E是代数域扩张K/F的一个中间域．K/F是纯不可分扩张必要且只要K/E和E/F都是纯不可分扩张．

证 因为$\iota(K/F)=\iota(K/E)\iota(E/F)$，所以，$\iota(K/F)=1$必要且只要$\iota(K/E)=\iota(E/F)=1$．于是由2.8.2就得到这个推论． ▮

推论 2.8.4 设F是一个特征为$p>0$的域．K是F的一个有限次纯不可分扩域．则

(i) $[K:F]=p^f$，f是一个非负整数；

(ii) 存在整数$e\geqslant 0$，使得

$$K^{p^e}=\{\alpha^{p^e}\mid \alpha\in K\}$$

是F的一个子域。

证 因为K是F的有限次扩域，所以存在F上代数元$\alpha_1,\cdots,\alpha_n\in K$，使得

$$K=F(\alpha_1,\cdots,\alpha_n).$$

因为K是F的纯不可分扩域，由2.8.2，对于每一个α_i，存在整数$e_i\geqslant 0$，使得$\alpha_i^{p^{e_i}}=a_i\in F$，所以$\alpha_i$是多项式$f_i(X)=X^{p^{e_i}}-a_i\in F[X]$的根。令$F_0=F$，$F_i=F(\alpha_1,\cdots,\alpha_i)=F_{i-1}(\alpha_i)$，那么$\alpha_i$在$F_{i-1}$上的最小多项式$g_i(X)$整除$f_i(X)$，所以$[F_i:F_{i-1}]=\deg(g_i(X))$也是$p$的一个幂。于是

$$[K:F]=\prod_{i=1}^{n}[F_i:F_{i-1}]=p^f.$$

这就证明了(i)成立。

(ii) 对于任意整数$e\geqslant 0$，$K\in\alpha\longmapsto\alpha^{p^e}\in K$是$K$到$K$内的一个同态单射，所以

$$K^{p^e}=\{\alpha^{p^e}\,|\,\alpha\in K\}$$

是K的一个子域。我们证明，对于足够大的e，将有$K^{p^e}\subseteq F$。

用证明(i)时所引入的记号，我们有扩域序列

$$F=F_0\subseteq F_1\subseteq\cdots\subseteq F_n=K,$$

$F_i=F_{i-1}(\alpha_i)$。我们证明，对于每个i，$1\leqslant i\leqslant n$，存在$e_i\geqslant 0$，使得$F_i^{p^{e_i}}\subseteq F_{i-1}$。如果这一事实被证明，那么取$e=e_1+e_2+\cdots+e_n$，则$K^{p^e}\subseteq F$，因此，问题就归结为证明以下论断：

设$K=F(\alpha)$，α是F上一个纯不可分元素。那么存在整数$e\geqslant 0$，使得$K^{p^e}\subseteq F$。

为了证明这个论断，我们注意到，由2.8.2，存在整数$e\geqslant 0$，使得$\alpha^{p^e}=a\in F$。$K=F(\alpha)$的任意元素γ总可以表示成

$$\gamma = \sum_{i=1}^{m} a_i \alpha^i, \quad a_i \in F.$$

于是

$$\gamma^{p^e} = \sum_{i=0}^{m} a_i^{p^e} (\alpha^{p^e})^i = \sum_{i=0} a_i^{p^e} a^i \in F.$$

所以$K^{p^e} \subseteq F$。 ▮

在这一节的最后，我们引入可分次数和不可分次数的概念。

设K是域F的一个代数扩域，S是F在K内的可分闭包。S在F上的次数$[S:F]$叫做K在F上的**可分次数**；K在S上的次数$[K:S]$叫做K在F上的**不可分次数**。

我们分别用$[K:F]_s$和$[K:F]_i$来表示K在F上的的可分次数和不可分次数，因此，当$[K:F]<\infty$时，我们有

$$[K:F]=[K:F]_s[K:F]_i.$$

并且有

$$K/F\text{可分} \Longleftrightarrow [K:F]=[K:F]_s.$$

令Ω是K的一个代数闭包。我们知道，当$[K:F]<\infty$时，K到Ω内的F-共轭的个数$\iota(K/F)$小于或等于域次数$[K:F]$(2.6.4)。下面的定理明说$\iota(K/F)$与可分次数$[K:F]_s$的关系。

定理 2.8.5 设K是域F的一个有限次扩域。那么

$$\iota(K/F)=[K:F]_s.$$

证 令S是F在K内的可分闭包，则K是S的纯不可分扩域。由2.8.2，$\iota(K/S)=1$。所以

$$\iota(K/F)=\iota(K/S)\iota(S/F)=\iota(S/F).$$

另一方面，S是F的有限次可分扩域，由2.7.6，

$$[K:F]_s=\iota(S/F).$$

因此。$\iota(K/F)=[K:F]_s$。 ▮

定理 2.8.6 设K是域F的一个有限次扩域，E是K/F的

一个中间域．那么

$$[K:F]_s=[K:E]_s[E:F]_s;$$
$$[K:F]_i=[K:E]_i[E:F]_i.$$

证 由2.8.5，我们有

$$[K:F]_s=\iota(K/F)=\iota(K/E)\iota(E/F)$$
$$=[K:E]_s[E:F]_s.$$

然而$[K:F]=[K:E][E:F]$．由此得出

$$[K:F]_i=[K:E]_i[E:F]_i.$$ ▮

习　　题

1. 写出定理2.8.2的证明．

2. 设K是域F的一个扩域，S是F在K内的可分闭包，P是K内一切在F上纯不可分元素所成的集，E是K/F的一个中间域．证明：

(i) K在E上是纯不可分的$\Longleftrightarrow S\subseteq E$；

(ii) 如果K在E上是可分的，则$P\subseteq E$；

(iii) 如果$E\cap S=F$，则$E\subseteq P$．

3. 设F是一个特征为$p>0$的域，α是F上一个代数元．证明，如果$F(\alpha)$在F上是纯不可分的，则$[F(\alpha):F]=p^e$，e是一个正整数．

4. 设$K=F_p(X,Y)$是p元素域F_p上不相关不定元X,Y的有理分式域，令$F=F_p(X^p,Y^p-Y)$．证明，$[K:F]=p^2$．确定F在K内的可分闭包S，并且求出$[K:F]_s$及$[K:F]_i$．

5. 设$K=F_p(X,Y)$是F_p上不相关不定元X,Y的有理分式域，$F=F_p(X^p-X,\ Y^p-Y)$．证明：

(i) K是F的p^2次可分扩域；

(ii) K中在F上纯不可分的元素都在F内．

2.9 完备域

我们已经对于可分扩域和不可分扩域的性质作了一些讨论．现在提出这样的问题：给了一个域 F，在什么的条件下，F 的每一个代扩域都是可分的？当 $\mathrm{char}F=0$ 时，这是不成为问题的，因为特征为 0 的域的任何代数扩域总是可分的．问题主要出在 $\mathrm{char}F=p>0$ 的情形．先给出以下定义．

一个域 F 说是**完备的**，如果 F 的每一个代数扩域都是可分的．这相当于说，$F[X]$ 的每一个不可约多项式都是可分的．事实上，如果 $F[X]$ 的每一个不可约多项式都可分，那么 F 上每一个代数元在 F 上的最小多项式是可分的，因而 α 是 F 上可分元素．反之，设 $f(X)$ 是 $F[X]$ 的一个不可约多项式，令 α 是 $f(X)$ 的一个根（在 F 的某一代数闭包内）．那么 α 在 F 上的最小多项式 $p(X)$ 是可分的，而 $f(X)$ 与 $p(X)$ 至多相差 F 中一个非零常数因子，所以 $f(X)$ 也是可分的．

由这个定义，注意到2.7.5，我们立即得到

定理 2.9.1 （i）特征为 0 的域是完备域．

（ii）有限域是完备域． ∎

定理 2.9.2 完备域的代数扩域还是完备域．

证 设 K 是完备域 F 的一个代数扩域．令 L 是 K 的任意一个代数扩域．L 也是 F 的代数扩域．所以 L 是 F 的可分扩域．再由 2.7.8，L 是 K 的可分扩域，所以 K 是完备的． ∎

现在设 F 是一个域，$\mathrm{char}F=p>0$，令 Ω 是 F 的一个代数闭包．对于任意非负整数 ν 定义

$$F^{p^\nu}=\{x^{p^\nu}\mid x\in F\};$$

$$F^{p^{-\nu}}=\{\alpha\mid \alpha\in\Omega,\ \alpha^{p^\nu}\in F\}.$$

容易验证，F^{p^ν} 和 $F^{p^{-\nu}}$ 都是 Ω 的子域，并且有

$$F\supseteq F^p\supseteq F^{p^2}\supseteq\cdots$$

$$F\subseteq F^{p^{-1}}\subseteq F^{p^{-2}}\subseteq\cdots\subseteq\Omega.$$

约定

$$F^{p^{-\infty}}=\bigcup_{\nu\geqslant 0}F^{p^{-\nu}},$$

则$F^{p^{-\infty}}$也是Ω的一个子域。

定理 2.9.3 设F是一个域，$\mathrm{char}F=p>0$。对于F来说，下列五个条件等价：

(i) F是完备域；

(ii) $F[X]$的每一个不可约多项式都是可分的；

(iii) $F^{p^{-\infty}}=F$；

(iv) $F^{p^{-1}}=F$；

(v) $F^{p}=F$。

证 (i)和(ii)显然等价。我们只证条件(i)，(iii)，(iv)，(v)的等价性。

(i)$\Longrightarrow$(iii) 如果$F^{p^{-\infty}}\supsetneqq F$，那么存在整数$\nu>0$，使得有$a\in F^{p^{-\nu}}$但$a\notin F$，而$a^{p^{\nu}}\in F$。所以$a$是$F$上纯不可分元素(2.7.4)。于是$F$的代数扩域$F(a)$是$F$的一个不可分扩域。

(iii)$\Longrightarrow$(iv) $F\subsetneqq F^{p^{-1}}\Longrightarrow F\subsetneqq F^{p^{-\infty}}$。

(iv)$\Longrightarrow$(v) $F^{p^{-1}}=F\Longleftrightarrow$对于任意$a\in F$，都有$b\in F$，使得$a=b^{p}\in F^{p}\Longleftrightarrow F^{p}=F$。

(v)$\Longrightarrow$(i) 如果F不是完备域，那么存在$a\in\Omega$，a在F上不可分。令$f(X)\in F[X]$是a在F上的最小多项式，则$f(X)$不可分。于是存在$g(X)\in F[X]$使得$f(X)=g(X^{p})$。令

$$g(X)=\sum_{i=0}^{m}b_iX^{i},\quad b_i\in F.$$

因为$F^{p}=F$，所以每一个系数都可以写成$b_i=a_i^{p}$的形式，$a_i\in F$ $(0\leqslant i\leqslant m)$。于是

$$f(X)=g(X^{p})=\sum_{i=0}^{m}b_iX^{ip}$$

$$= \sum_{i=0}^{m} a_i^p X^{ip} = \left(\sum_{i=1}^{m} a_i X^i\right)^p$$

这与 $f(X)$ 的不可约性相违。 ▮

推论 2.9.4 设 F 是一个特征为 $p>0$ 的域。则 $F^{p^{-\infty}}$ 是完备域。

证 设 $\alpha \in F^{p^{-\infty}}$。那么存在一个整数 $\nu \geqslant 0$ 使得 $\alpha \in F^{p^{-\nu}}$。令 β 是多项式 $X^p - \alpha$ 的一个根（在 $F^{p^{-\infty}}$ 的某一代数闭包内）。则

$$\beta \in F^{p^{-(\nu+1)}} \subseteq F^{p^{-\infty}}, \text{ 且 } \beta^p = \alpha.$$

所以

$$(F^{p^{-\infty}})^p = F^{p^{-\infty}}.$$

由 2.9.3，(v)，$F^{p^{-\infty}}$ 是完备的。 ▮

习　题

1. 设 K 是域 F 的一个有限次扩域。证明，K 是完备域必要且只要 F 是完备域。

2. 设 F 是一个特征为 $p>0$ 的非完备域，$a \in F$ 但 $a \notin F^p$。证明，多项式 $X^{p^e} - a$ 在 $F[X]$ 中不可约，这里 e 是一个非负整数。

3. 设 F 是一个特征为 $p>0$ 的域，t 是 F 上一个超越元。证明 $F(t)$ 不是完备域。

4. 设 F 是一个特征为 $p>0$ 的域。证明：

(i) $F^{p^{-\infty}}$ 是包含 F 的最小完备域；

(ii) 对于每一个正整数 ν 来说，$F^{p^{-\nu}}$ 与 F 同构，但 $F^{p^{-\infty}}$ 不一定与 F 同构。

2.10 本原元素定理

我们证明域的有限次可分扩域的一个重要的性质来结束这一章。

先证明关于单代数扩域的一个性质.

定理 2.10.1 令K是域F的一个扩域. 那么K是F的一个有限次单扩域必要且只要K/F只有有限个中间域.

证 如果K是F的有限次单扩域, 那么存在K的一个元素α,使得$K=F(\alpha)$,并且α是F上的代数元. 令$f(X)$是α在F上的最小多项式. 设E是K/F的一个中间域, 那么α在E上也是代数的. 令$f_E(X)\in E[X]$是α在E上的最小多项式. 我们有$f_F(X)=f(X)$, $f_K(X)=X-\alpha$. $f_E(X)$是由中间域E唯一确定的. 令

$$\mathfrak{M}=\{E\mid E\text{是}K/F\text{的中间域}\}.$$

$$\mathfrak{N}=\{f_E(X)\mid f_E(X)\text{是}\alpha\text{在}E\text{上的最小多项式}, E\in\mathfrak{M}\}.$$

那么$E\longmapsto f_E(X)$是$\mathfrak{M}$到$\mathfrak{N}$的满射. 我们证明, 这个映射是双射. 事实上, 设$E_1,E_2\in\mathfrak{M}$. 如果

$$f_{E_1}(X)=f_{E_2}(X)=g(X).$$

令$L=E_1\cap E_2$. 则$g(X)\in E_1[X]\cap E_2[X]=L[X]$. $g(X)$是$E_1[X]$的不可约多项式, 自然也是$L[X]$的不可约多项式. 因为$g(\alpha)=0$, 所以$g(X)$是α在L上最小多项式: $g(X)=f_L(X)$. 另一方面, $K=F(\alpha)$而$F\subseteq L\subseteq E_i\subseteq K$, 所以

$$K=L(\alpha)=E_i(\alpha),\quad i=1,2.$$

又$[K:E_i]=\deg(f_{E_i}(X))=\deg(g(X))=[K:L]$, 所以

$$[E_i:L]=[K:L]/[K:E_i]=1,i=1,2.$$

于是$E_1=L=E_2$. 这就证明了映射$E\longmapsto f_E(X)$是集$\mathfrak{M}$到$\mathfrak{N}$集的双射.

$\mathfrak{N}$是有限集, 因为对于任意中间域E, 多项式$f_E(X)$整除$f(X)$, 而$f(X)$的最高次项系数是1的非常数因式只有有限多个. 因此$\mathfrak{N}$是有限集.

反之, 设K/F只有有限个中间域. 我们首先证明, K是F的代数扩域. 事实上, 如果K含有F上的一个超越元x, 那么x^2

也是 F 上超越元，并且 $F(x)\supsetneqq F(x^2)$。这样一来，K/F 含有无限多个中间域

$$K\supseteq F(x)\supsetneqq F(x^2)\supsetneqq F(x^4)\supsetneqq\cdots\supsetneqq F(x^{2^n})\supsetneqq\cdots\supsetneqq F.$$

与题设矛盾.

其次，K 是 F 上有限个代数元生成的扩域. 因为如果不然的话，必定存在一个扩域的无限序列，

$$F\subsetneqq F(\alpha_1)\subsetneqq F(\alpha_1,\alpha_2)\subsetneqq\cdots\subsetneqq F(\alpha_1,\cdots,\alpha_n)\subsetneqq\cdots\subsetneqq K.$$

这又与题设矛盾.

这样，K 是 F 上有限个代数元生成的扩域，因而是 F 的有限次扩域.

我们证明 K 是 F 的单扩域. 如果 F 是有限域，那么由2.4.10，K 是 F 的单扩域. 现在设 F 是无限域. 对于任意 $a\in K$，我们有

$$[F(a):F]\leqslant[K:F]<\infty.$$

又因为 K/F 只有有限中间域，所以

$$\{[F(a):F]\mid a\in K\}$$

是自然数的有限集，因此存在 $\theta\in K$，使得对于任意 $a\in K$ 都有

$$[F(\theta):F]\geqslant[F(a):F].$$

考虑 K 中任意元素 β. 对于任意 $c\in F$，令

$$E_c=F(\beta+c\theta).$$

则 $F\subseteq E_c\subseteq K$. 由假设，这样的 E_c 只有有限多个. 然而 F 含有无限多个元素，因此必存在 $c_1,c_2\in F,c_1\neq c_2$，而 $E_{c_1}=E_{c_2}==E$. 因为 $\beta+c_1\theta$，$\beta+c_2\theta\in E$，所以 $\theta\in E$. 于是

$$F(\theta)\subseteq E=F(\beta+c_1\theta).$$

所以

$$[F(\theta):F]\leqslant[F(\beta+c_1\theta):F].$$

由 θ 的取法，必须等号成立，从而

$$F(\theta)=E=F(\beta+c_1\theta).$$

由此得出，$\beta=(\beta+c_1\theta)-c_1\theta\in F(\theta)$. 这样一来，$K$ 中任意

元素 β 都属于 $F(\theta)$，从而 $K=F(\theta)$。 ∎

我们现在证明以下的所谓本原元素定理。

定理 2.10.2 设 $K=F(\alpha_1,\cdots,\alpha_s,\beta)$ 是域 F 的一个代数扩域，其中 $\alpha_1,\cdots,\alpha_s$ 都是 F 上的可分元素。那么 K 是 F 的一个单扩域。

证 如果 F 是有限域，那么由2.4.10，定理成立。设 F 是无限域。先看 $s=1$ 的情形。这时 $K=F(\alpha,\beta)$，α,β 是 F 上代数元且 α 在 F 上可分。令 Ω 是 K 的一个代数闭包。令

$$m=\iota(K/F)=[K:F]_s,$$

设 $\sigma_i: K\longrightarrow\Omega\ (1\leqslant i\leqslant m)$ 是 K 到 Ω 内的一切互不相同的 F-共轭映射。那么当 $i\neq j$ 时，或者 $\sigma_i(\alpha)\neq\sigma_j(\alpha)$，或者 $\sigma_i(\beta)\neq\sigma_j(\beta)$。因为 F 是无限域，所以对于一切数对 (i,j)，$1\leqslant i\leqslant m$，$i\neq j$，总可以找到 F 的一个元素 c，使得

$$(\sigma_i(\alpha)-\sigma_j(\alpha))+c(\sigma_i(\beta)-\sigma_j(\beta))\neq 0.$$

令 $\theta=\alpha+c\beta$。则 $\theta\in K$，所以 $F\subseteq F(\theta)\subseteq K$。由 c 的取法可知当 $i\neq j$ 时，$\sigma_i(\theta)\neq\sigma_j(\theta)$。因此，$\sigma_i$ 在 $F(\theta)$ 上的限制 $\sigma_i|_{F(\theta)}$ $(i=1,2,\cdots,m)$ 是 $F(\theta)$ 到 Ω 内的 m 个互不相同的 F-共轭。于是

$$[K:F]_s=\iota(K/F)\leqslant\iota(F(\theta)/F)=[F(\theta):F]_s.$$

另一方面，因为 $F\subseteq F(\theta)\subseteq K$，所以

$$[F(\theta):F]_s\leqslant[K:F]_s.$$

因此必须

$$[F(\theta):F]_s=[K:F]_s.$$

这就是说，F 在 $F(\theta)$ 内的可分闭包与 F 在 K 内的可分闭包重合。令 S 表示这个可分闭包。那么 $\alpha\in S\subseteq F(\theta)$，从而 $\beta=c^{-1}(\theta-\alpha)\in F(\theta)$。这样一来。$K=F(\alpha,\beta)\subseteq F(\theta)$，即 $K=F(\theta)$。

设 $s\geqslant 2$，$K=F(\alpha_1,\cdots,\alpha_s,\beta)$，其中 $\alpha_1,\cdots,\alpha_s$ 都是 F 上可分元素。由归纳法假设，存在 $\gamma\in K$ 使得 $K'=F(\alpha_1,\cdots,\alpha_{s-1},\beta)=F(\gamma)$。于是 $K=K'(\alpha_s)=F(\alpha_s,\gamma)$，这就归结到前一个情

形。因此存在 $\theta\in K$ 使 $K=F(\theta)$。 ∎

由这个定理，立即得出以下两个推论：

推论 2.10.3 设 K 是域 F 的一个有限次可分扩域，则 K 是 F 上的单扩域。 ∎

推论 2.10.4 设 K 是域 F 的一个有限次可分扩域，则 K/F 只有有限个中间域。 ∎

由本原元素定理，我们可以对于代数闭包用一个较弱的条件来刻画。

定理 2.10.5 设 K 是域 F 的一个代数扩域。对于 K 来说，以下两个条件是等价的：

(i) K 是 F 的代数闭包；

(ii) $F[X]$ 的每一个次数大于零的多项式在 K 中有一个根。

证 (i)$\Longrightarrow$(ii) 是明显的。

(ii)$\Longrightarrow$(i) 令 Ω 是 K 的一个代数闭包。则 Ω 自然也是 F 的代数闭包。我们证明 $\Omega=K$。分两个情形讨论。

(a) $\operatorname{char}F=p>0$。设 $\alpha\in\Omega$。令 $f(X)$ 是 α 在 F 上最小多项式。于是存在非负数 e 和 F 上一个不可约的可分多项式 $g(X)$ 使得 $f(X)=g(X^{p^e})$。$g(X)$ 在 $\Omega[X]$ 内分解成一次因式乘积：

$$g(X)=\prod_{i=1}^{m}(X-\beta_i),$$

这里 $\beta_1,\cdots,\beta_m$ 是 Ω 中两两不同的可分元素。于是由 2.10.2，$L=F(\beta_1,\cdots,\beta_m)$ 是 F 上的单扩域，即存在 $\theta\in L$ 使得 $L=F(\theta)$。然而

$$0=f(\alpha)=g(\alpha^{p^e})=\prod_{i=1}^{m}(\alpha^{p^e}-\beta_i),$$

所以 α^{p^e} 必定等于某一个 β_i，从而 $\alpha^{p^e}\in L$。

令 $h(X)$ 是 θ 在 F 上的最小多项式，则 $h(X^{p^e})$是 $F[X]$ 的一个次数大于零的多项式. 由(ii)，$h(X^{p^e})$ 在K里有一个根 γ. 令 $\theta_1=\gamma^{p^e}$，则 $h(\theta_1)=0$. 由2.2.7，存在Ω的一个F-自同构ω，使得 $\omega(\theta)=\theta_1$，从而 $L=F(\theta)$与$F(\theta_1)$是 F-共轭的. 然而 L 是 $g(X)$在 F 上的分裂域，因而是 F 的正规扩域，因此 $L=F(\theta_1)$. 这样就得出$\alpha^{p^e}=\beta_i\in L=F(\theta_1)$. 所以

$$\alpha^{p^e}=\sum_{j=0}^{s}a_j\theta_1^j,\quad a_j\in F.$$

由(ii)，每一个多项式$X^{p^e}-a_j\in F[X]$在K里有一个根α_j，$0\leqslant j\leqslant s$，因此

$$\alpha^{p^e}=\sum_{j=0}^{s}a_j\theta_1^j=\sum_{j=0}^{s}\alpha_j^{p^e}(\gamma^{p^e})^j=\left(\sum_{j=0}^{s}\alpha_j\gamma^j\right)^{p^e}.$$

所以

$$\alpha=\sum_{j=0}^{s}\alpha_j\gamma^j\in K.$$

这就证明了 $\Omega\subseteq K$ 从而$K=\Omega$是 F 的代数闭包.

(b) 设char$F=0$. 设$\alpha\in\Omega$. 令$f(X)$是 α在F上的最小多项式. 则$f(X)$在$\Omega[X]$中可以分解成一次因式的乘积：

$$f(X)=\prod_{i=1}^{n}(X-\alpha_i),\quad \alpha_i\in\Omega.$$

并且当 $i\neq j$ 时，$\alpha_i\neq\alpha_j$. 令 $L=F(\alpha_1,\cdots,\alpha_n)$. 则 $\alpha\in L$. 由2.10.2，$L=F(\theta)$，θ是L中一个元素，令 $h(X)$ 是θ在F上的最小多项式. 由(ii)，$h(X)$在K里有一个根 θ_1. 又因为L是$f(X)$在F上的分裂域，因而是正规扩域. 由此推出$L=F(\theta_1)$. 这样就有 $\alpha\in L=F(\theta_1)\subseteq K$，从而$K=\Omega$. ∎

由于 $F[X]$中每一个次数大于零的的多项式都是 $F[X]$的一些不可约多项式的乘积，我们立即得到

推论 2.10.6 对于域F的一个代数扩域K来说，以下两个条件是等价的：

（i） K是F的代数闭包；

（ii） $F[X]$的每一个不可约多项式在K中有一个根． ∎

习　题

1. 设K是域F的一个n次单扩域．证明，K/F的中间域的个数至多等于2^n-1．

2. 设K是域F的有限次可分扩域，Ω是K的代数闭包，$\alpha\in K$．证明以下两条件是等价的：

（i） α是K在F上一个本原元素，即$K=F(\alpha)$；

（ii） 在Ω内，α在F上的共轭元素的个数等于$[K:F]$．

3. 令k是一个特征为$p>0$的域，$F=k(t_1,t_2)$是k上不相关不定元t_1,t_2的有理分式域，Ω是F的一个代数闭包，α_1，α_2分别是X^p-t_1和$X^p-t_2\in F[X]$在Ω内的根．令$K=F(\alpha_1,\alpha_2)$．证明：

（i） $[K:F]=p^2$，且K/F是不可分扩张；

（ii） 对于任意$\alpha\in K$，都有$[F(\alpha):F]\leqslant p$；

（iii） K不是F上的单扩域；

（iv） K/F有无限多个中间域．

4. 设K是域F上一个可分扩域．证明，如果K中每一个元素在F上的最小多项式的次数都有一个共同的上界N，那么K/F是有限次扩张，且$[K:F]\leqslant N$．

第三章　Galois理论

Galois 理论主要是在一个特定的域扩张K/F的中间域所组成的集与K的 F- 自同构群的子群所组成的集之间建立了一个双射。这样就使得域论问题的研究可以归为群论问题，从而得到域论中一些较为深刻的结果。

3.1　Galois 扩域

设K是一个域。令 $\mathrm{Aut}(K)$ 表示K的一切自同构所组成的集。设 $\sigma,\tau\in\mathrm{Aut}(K)$，那么合成映射 $\sigma\circ\tau$ 仍是K的一个自同构。我们定义 σ 与 τ 的积$\sigma\tau=\sigma\circ\tau$，即对于任意 $a\in K$，

$$\sigma\tau(a)=\sigma(\tau(a))。$$

这样定义的乘法自然满足结合律。恒等自同构 1_K 是单位元。又K的每一个自同构σ有逆σ^{-1}，并且 σ^{-1}也是K的自同构。这样，$\mathrm{Aut}(K)$ 对于如上定义的乘法作成一个群，称为K的全体自同构群。

设F是域K的一个子域。令

$$G(K/F)=\{\sigma\in\mathrm{Aut}(K)\,|\,\sigma(a)=a,\ \forall a\in F\}.$$

$G(K/F)$就是K的一切F-自同构所组成的集。它是 $\mathrm{Aut}(K)$的一个子群，称为K的**F-自同构群**

反过来设G是$\mathrm{Aut}(K)$的一个子群。令

$$K^G=\{a\in K\,|\,\sigma(a)=a,\ \forall\sigma\in G\}.$$

那么K^G是K的一个子域，称为群G的**固定域**。

现在给定一个域K。设F是K的一个子域。H是$\mathrm{Aut}(K)$ 的一个子群。记 $G(F)=G(K/F)$是K的 F-自同构群；K^H 是子群

H的固定域。又记 $1=1_K$。我们有以下事实：

1. $F\subseteq K^{G(F)}$。

2. $H\subseteq G(K^H)$。

3. F_1，F_2 是K的子域，且$F_1\subseteq F_2$，则$G(F_1)\supseteq G(F_2)$；$G(K)=\{1\}$。

4. H_1，H_2是$\mathrm{Aut}(K)$的子群，且$H_1\subseteq H_2$则 $K^{H_1}\supseteq K^{H_2}$；$K^{\{1\}}=K$。

5. $G(F)=G(K^{G(F)})$。

这些事实的证明都是非常容易的。我们只证 5。

由 1，$F\subseteq K^{G(F)}$。再由 3，

$$G(F)\supseteq G(K^{G(F)})。$$

另一方面，由 2，

$$G(F)\subseteq G(K^{G(F)})。$$

所以

$$G(F)=G(K^{G(F)})。$$

例 1 设 $F=\mathbf{Q}$ 是有理数域，$K=\mathbf{Q}(\sqrt[3]{2})$。那么 $G(F)=G(K/F)=\{1\}$，从而$K^{G(F)}=K$。

例 2 设$F=\mathbf{F}_p(x)$是 p 元有限域 $\mathbf{F}_p$上不定元 x 的有理分式域；$K=F(x^{1/p})$。那么K是 F 的一个纯不可分扩域。所以K只有唯一的F-自同构——恒等自同构 1 。因此$G(F)=\{1\}$，而$K^{G(F)}=K\supsetneqq F$。

以上两个例子告诉我们，1 中的包含关系可能是真包含关系。在Galois 理论中，主要是讨论这样的域扩张K/F，其中$F=K^{G(F)}$。

定理 3.1.1 设K是域F的一个代数扩域。对于K来说，下列三个条件是等价的：

(i) K是F的一个可分正规扩域；

(ii) $F=K^{G(F)}$；

(iii) 存在$G(F)$的一个子群G，使得$F=K^G$.

证 (i)$\Longrightarrow$(ii) 我们只需证明$K^{G(F)}\subseteq F$. 设$\alpha\in K$但$\alpha\notin F$. 令$f(X)$是α在F上的最小多项式. 由(i)，$f(X)$在$K[X]$内分解成两两互素的一次因子的乘积：

$$f(X)=\prod_{i=1}^{n}(X-\alpha_i),$$

这里$\alpha_i\in K$，且$\alpha_1,\alpha_2,\cdots,\alpha_n$两两不同. 令$\alpha_1=\alpha$. 因为$\alpha\notin F$，所以$n=\deg(f(X))>1$. 所以有$\alpha_2\in K$，$\alpha_2\neq\alpha$，由2.3.3，存在$\sigma\in G(F)$使得$\sigma(\alpha)=\alpha_2\neq\alpha$. 所以$\alpha\notin K^{G(F)}$.

(ii)$\Longrightarrow$(iii) 由(ii)，取$G=G(F)$即可.

(iii)$\Longrightarrow$(i) 设有$G(F)$的一个子群G，使得$F=K^G$. 对于任意$\alpha\in K$，令$f(X)$是α在F上的最小多项式. 那么对于任意$\sigma\in G\subseteq G(F)$，我们有

$$f(\sigma(\alpha))=\sigma(f(\alpha))=0.$$

所以$\sigma(\alpha)$也是$f(X)$在K内的一个根. 然而$f(X)$在K内只有有限个根，所以

$$\sum_\alpha=\{\sigma(\alpha)\mid\sigma\in G\}$$

是有限集，设$\sum_\alpha=\{\alpha_1,\cdots,\alpha_n\}$，$\alpha_i\neq\alpha_j$，若$i\neq j$. 那么对于任意$\tau\in G$，$\tau(\alpha_1),\cdots,\tau(\alpha_n)$仍是$f(X)$在$K$内两两不同的根，从而

$$\sum_\alpha=\{\tau(\alpha_1),\cdots,\tau(\alpha_n)\}.$$

令

$$g(X)=\prod_{i=1}^{n}(X-\alpha_i).$$

$g(X)$的系数是$\alpha_1,\cdots,\alpha_n$的对称多项式，所以在τ的作用下保持不动，从而属于$K^G=F$. 这样$g(X)\in F[X]$，因为$\alpha\in\sum_\alpha$，所以$g(\alpha)=0$，因而$g(X)$可以被α在F上的最小多项式$f(X)$整除. 于是在$K[X]$里，$f(X)$可以分解成两两互素的一次因式

的乘积．由2.3.2，K是F的一个正规扩域．$f(X)$是F上可分多项式．所以α是F上可分元素，因而K是F的一个可分正规扩域．∎

定义 设K是域F的一个代数扩域，如果K满足3.1.1中三个等价的条件之一，就称K是F的一个 **Galois 扩域**；这时K/F称为一个 **Galois 扩张**；K的F-自同构群$G(F)=G(K/F)$称K/F的 **Galois 群**．

定理 3.1.2 设K是域F的一个扩域．对于K来说，以下两个条件是等价的：

（i） K是F的有限次 Galois 扩域；

（ii） K是$F[X]$中一些可分的不可约多项式$f_1(X)$，…，$f_s(X)$的幂的乘积

$$f(X)=\prod_{i=1}^{s}f_i(X)^{e_i},e_i\geqslant 1,1\leqslant i\leqslant s,$$

在F上的一个分裂域．

证 (i)$\Longrightarrow$(ii) K是F上有限次正规扩域．由2.3.5，K是$F[X]$中一个多项式$f(X)$在F上的分裂域．可设$f(X)$最高次项系数是1．在$F[X]$内，$f(X)$分解成不可约多项式幂的乘积：

$$f(X)=\prod_{i=1}^{s}f_i(X)^{e_i},$$

$f_i(X)\in F[X]$是最高次项系数为1的不可约多项式，$e_i\geqslant 1$，$i=1,\cdots,s$．因为在$K[X]$内，$f(X)$可以分解成为一次因式的积，所以每一个$f_i(X)$在$K[X]$内也可以分解成为一次因式的积：

$$f_i(X)=\prod_{j=1}^{n_i}(X-\alpha_{ij}),$$

$\alpha_{ij}\in K$，$1\leqslant j\leqslant n_i$，$1\leqslant i\leqslant s$．$f_i(X)$是$K$的元素$\alpha_{ij}$在$F$上的

最小多项式．因为K是F的可分扩域，所以α_{ij}是F上可分元素，即$f_i(X)$是F上可分多项式，$1\leqslant i\leqslant s$.

(ii)$\Longrightarrow$(i)　我们有

$$f(X)=a\prod_{i=1}^{n}(X-\alpha_i),$$

$a\in F,\alpha_i\in K,1\leqslant i\leqslant n$；$K=F(\alpha_1,\cdots,\alpha_n)$．由2.3.5，$K$是$F$的有限次正规扩域．因为每一个$\alpha_i$都是$F[X]$中某一个可分的不可约多项式的根，所以$\alpha_i$是$F$上可分元素．由2.7.6，$K$是$F$上一个可分扩域，这样，$K$就是$F$上一个有限次 Galois 扩域．▮

因为特征为 0 的域的每一扩域都是可分的，所以立即得到

推论 3.1.3　设 char$F=0$．K是域F的一个有限次 Galois 扩域当且仅当K是$F[X]$的某一个多项式的分裂域．▮

定理 3.1.4　设K是域F的一个有限次扩域．对于K来说，以下两条件是等价的：

(i)　K是F的一个Galois扩域；

(ii)　群$G(K/F)$的阶等于域次数$[K:F]$.

证　(i)$\Longrightarrow$(ii)　令Ω是K的一个代数闭包．因为K是F的 Galois 扩域，所以是正规扩域．因此对于K的任意F-共轭$\sigma:K\to\Omega$来说，都有$\sigma(K)=K$，从而$\sigma\in G(K/F)$．因为K是F的可分扩域，所以

$$|G(K/F)|=\iota(K/F)=[K:F].$$

(ii)$\Longrightarrow$(i)　令$E=K^{G(K/F)}$．则$F\subseteq E\subseteq K$，由3.1.1(ii)，K是E的 Galois 扩域．由本节开始时所述的事实 5，我们有

$$G(K/E)=G(K/F).$$

这样一来，可以对于 Galois 扩张K/E应用(i)$\Longrightarrow$(ii)．于是我们有

$$|G(K/F)|=|G(K/E)|=[K:E]\leqslant[K:F].$$

另一方面，我们已知$|G(K/F)|=[K:F]$．这样就有$[K:E]$

$=[K:F]$，从而$E=F$。即K是F的Galois扩域。 ▮

定理 3.1.5 设K是域F的一个有限次可分扩域；Ω是F的一个包含K的代数闭包。那么存在Ω的一个子域L，它满足以下条件：

（i） $F\subseteq K\subseteq L\subseteq \Omega$，并且$L/F$是有限次Galois扩张；

（ii） 如果$N\subseteq \Omega$是F的一个包含K的Galois扩域，那么$L\subseteq N$。

证 因为K是F的有限次可分扩域，所以由2.10.3，$K=$ $=F(\alpha)$是F的一个单扩域。α在F上最小多项式$f(X)$是可分的。令$L\subseteq\Omega$是$f(X)$在F上的分裂域。由3.1.2，L是F的有限次Galois扩域，并且

$$F\subseteq K\subseteq L\subseteq \Omega.$$

设$N\subseteq\Omega$是F的任意一个Galois扩域，且$N\supseteq K$。则$\alpha\in K\subseteq N$。因为N是F上正规扩域，所以由2.3.2，$f(X)$在$N[X]$中可以分解成为一次因式的积：

$$f(X)=\prod_{i=1}^{n}(X-\alpha_i),\quad \alpha_i\in N.$$

因此$L=F(\alpha_1,\cdots,\alpha_n)\subseteq N$。

注1. 由(ii)立即推出L是唯一确定的。 ▮

2. 设$[K:F]=n$。则$G=G(L/F)$是集合$\{\alpha_1,\cdots,\alpha_n\}$上的一个置换群。设$\sigma\in G,\sigma(\alpha_i)=\alpha_{\nu_i}, 1\leqslant i\leqslant n$。因为$L=F(\alpha_1,\cdots,\alpha_n)$，所以

$$G\ni\sigma\longmapsto\begin{pmatrix}1 & 2 & \cdots & n\\ \nu_1 & \nu_2 & \cdots & \nu_n\end{pmatrix}\in S_n$$

是一个群同态单射，这里S_n表示n次对称群。因而G同构于S_n的一个子群。于是$[L:F]=|G|$是$n!$的一个因数。

由定理3.1.5，对于域F的一个有限次可分扩域$K(\subseteq\Omega)$，由条件(i)，(ii)所唯一确定的有限次Galois扩域L称为扩张

K/F的 Galois 闭包。

定理 3.1.6 设E是域扩张 K/F 的一个中间域。如果K/F是Galois 扩张，则K/E也是 Galois 扩张。

证 K是F上可分扩域，所以也是E上可分扩域。设K'是K在E上任意一个共轭域。那么在K和K'的一个共同的扩域M内，存在K到K'的一个E-同构φ。因为$E\supseteq F$，所以φ也是一个F-同构。因而K与K'是F-共轭的。因为K是F的正规扩域，所以 $K'=\varphi(K)=K$。因此K也是E的正规扩域。这样，K/E是可分正规扩张，从而是 Galois 扩张。 ∎

注意 E/F一般不是Galois 扩张。参看下一节例 4 和例 5。

定理 3.1.7 设K是域F的一个正规扩域；$G=G(K/F)$是K的一切F-自同构所成的群；K^G是G在K中的固定域。又设K_s是F在K内的可分闭包，K_i是K中一切在F上纯不可分元素的集。那么

(i) $K^G=K_i$，从而K_i是K的一个包含F的子域；

(ii) K是K_i上的 Galois 扩域，K/K_i的 Galois 群就是G；

(iii) $K=K_sK_i$，$K_s\cap K_i=F$。

证 令Ω是K的一个代数闭包。

(i) 由2.7.4 (iii)，$\alpha\in K_i$当且仅当对于K到Ω内的任意一个F-共轭φ来说，都有 $\varphi(\alpha)=\alpha$。然而K是F的正规扩域，因此K到Ω的每一个F-共轭φ都是K的F-自同构，即$\varphi\in G(K/F)=G$。因此 $\alpha\in K_i$当且仅当对于任意 $\varphi\in G$，都有$\varphi(\alpha)=\alpha$，也就是说，当且仅当 $\alpha\in K^G$。所以$K^G=K_i$。

(ii) 由(i)，我们有

$$G(K/K_i)=G(K_i)=G(K^G)=G.$$

(iii) K/K_s是纯不可分扩张。由2.8.3，K/K_sK_i也是纯不可分扩张。然而由(ii)，K/K_i是可分扩张，所以由2.7.8，

K/K_sK_i也是可分扩张。因此必须$K=K_sK_i$。

最后，$K_s\cap K_i$中任意元素α既在F上可分又在F上不可分，所以$\alpha\in F$，从而$K_s\cap K_i=F$。 ∎

推论 3.1.8 设K是域F上一个有限次正规扩域。那么

$$[K:K_i]=[K_s:F],\quad [K:K_s]=[K_i:F].$$

证 由3.1.7，K/K_i是有限次Galois扩张，它的Galois群是$G(K/K_i)=G(K/F)$。于是由3.1.4和2.8.5，

$$[K:K_i]=|G(K/F)|=\iota(K/F)=[K_s:F].$$

于是

$$[K:K_s]=[K:F]/[K_s:F]=[K:F]/[K:K_i]$$
$$=[K_i:F].$$ ∎

最后我们再给出有关扩域的合成域的一个定理。

定理 3.1.9 设K是域F的一个Galois扩域，L是F的任意扩域，并且假设K和L都被包含在某一个共同的扩域内。则

(i) KL是L的Galois扩域；

(ii) 如果$[K:K\cap L]<\infty$，则

$$[KL:L]=[K:K\cap L],$$

并且

$$G(KL/L)\cong G(K/K\cap L).$$

证 (i) 因为K是F的可分扩域，所以K的每一个元素也在$L\supseteq F$上可分。由2.7.7，$KL=L(K)$是L上可分扩域。

令σ是KL的任意一个L-共轭。则σ在K上的限制$\sigma|_K$自然是K的一个F-共轭。因为K/F是正规扩张，所以$\sigma(K)=K$。因为KL的每一个元素都是K和L的元素的积的组合，所以$\sigma(KL)=KL$。因此KL是L的正规扩域。

这样，KL是L的Galois扩域。

(ii) 令$E=K\cap L$。由3.1.6，K/E也是有限次Galois扩张，因而是有限次可分扩张。于是由2.10.3，存在$\alpha\in K$，使

得$K=E(\alpha)$．设$f(X)$是α在E上的最小多项式．因为K是E的正规扩域，所以由2.3.2，在$K[X]$内，

$$f(X)=(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n),$$

$\alpha_i\in K, 1\leqslant i\leqslant n, \alpha=\alpha_1$．另一方面，$\alpha$也是$L$上代数元，且$KL=LE(\alpha)=L(\alpha)$．令$g(X)$是$\alpha$在$L$上的最小多项式．那么在$L[X]$内，$g(X)\mid f(X)$．所以$g(X)$的根都是$f(X)$的根，因而属于$K$．于是$g(X)$的系数作为根的初等对称多项式，都属于$K$，从而属于$E=K\cap L$．这样一来就必须有$f(X)=g(X)$．因此

$$[KL:L]=\deg(g(X))=\deg(f(X))=[K:E].$$

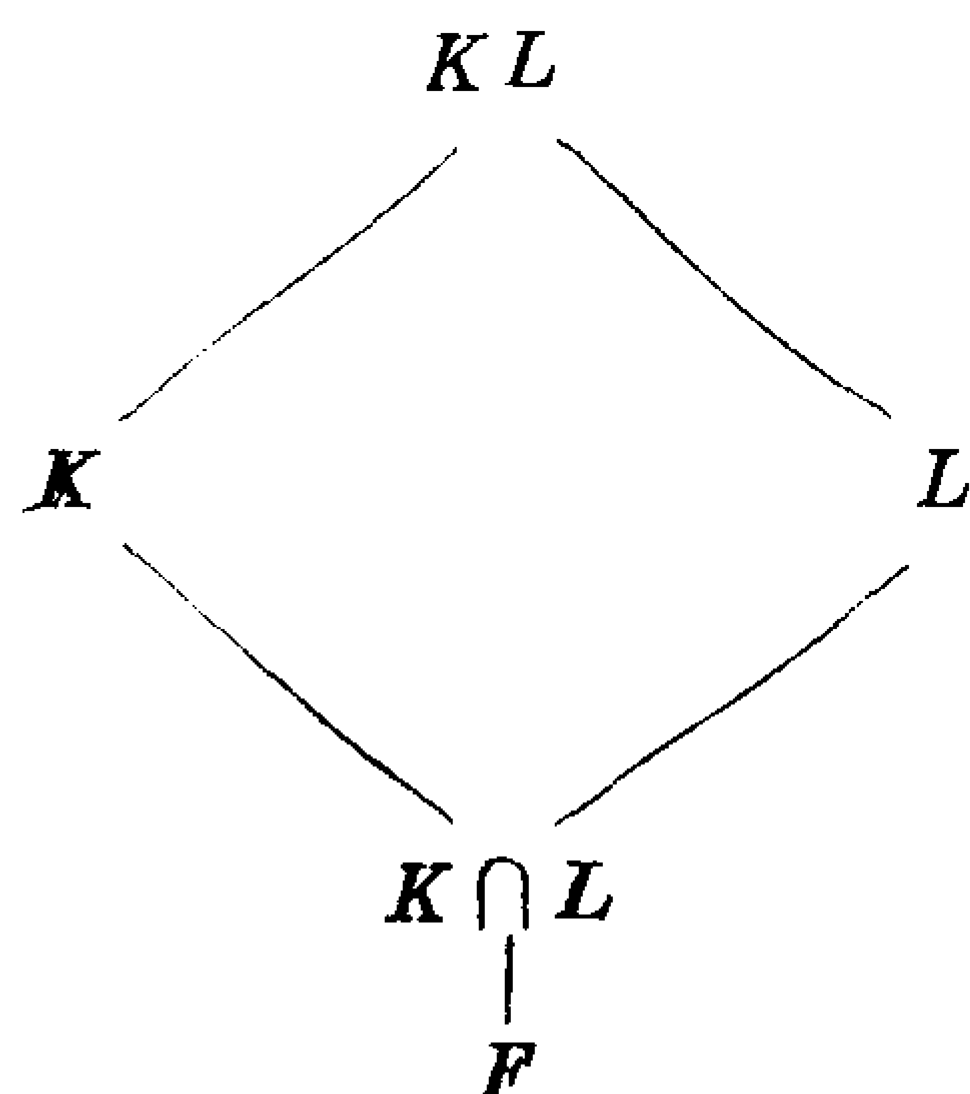
现在设$\sigma\in G(KL/L)$．那么$\sigma|_K$自然使$E=K\cap L$的元素保持不动，所以$\sigma|_K\in G(K/E)$．这样，

$$\theta: G(KL/L)\ni\sigma\longmapsto\sigma|_K\in G(K/E)$$

是群$G(KL/L)$到群$G(K/E)$的同态映射．如果$\sigma\in G(KL/L)$而$\sigma|_K=1_K$，则显然$\sigma=1_{KL}$．因而θ是单射．最后再由3.1.4和上面所证明的事实，我们有

$$|G(KL/L)|=[KL:L]=[K:E]=|G(K/E)|.$$

所以 $\quad G(KL/L\cong)G(K/E)=G(K/K\cap L)$． ∎



定理 3.1.9 可以用左边的图来示意．

注意，在上面定理的证明里，K/F是Galois扩张这一条件是必要的．当K和L都不是F的Galois扩域时，定理一般不成立．例如令$K=Q(\sqrt[3]{2})$，$L=Q(\zeta\sqrt[3]{2})$，$\zeta=e^{2\pi i/3}$．则$K\cap L=Q$，$KL=Q(\sqrt[3]{2},\sqrt{-3})$，我们有$[KL:Q]=6$，$[L:Q]=3$，以所$[KL:L]=2$．然而$[K:K\cap L]=[K:Q]=3$．（参看3.2，例4.）

习　题

1. 设 m，n 是不含平方因子的不同的整数，$K=\mathbf{Q}(\sqrt{m},\sqrt{n})$，证明，$K/\mathbf{Q}$ 是 Galois 扩张．确定 Galois群$G(K/\mathbf{Q})$．

2. 设$E=\mathbf{Q}(\sqrt{2})$，$K=\mathbf{Q}(\sqrt[4]{2})$．证明$K/E$和$E/\mathbf{Q}$ 都是 Galois 扩张．$K/\mathbf{Q}$是不是 Galois 扩张?

3. 设 k 是一个特征为 $p>0$ 的域，t 是 k 上一个超越元．$K=k(t)$，$F=(t^p-t)$．证明，K/F 是一个 Galois 扩张，且 $G(K/F)\cong\mathbf{Z}/(p)$（以 p 为模的剩余类加群）．

4. 设$K_\lambda(\lambda\in\Lambda)$都是域$F$的 Galois 扩域．令$K=\bigcap_{\lambda} K_\lambda$．证明$K$也是 F 的Galois的扩域．

5. 证明，实数域$\mathbf{R}$只有唯一的自同构——恒等自同构．

［提示：设$\sigma\in\mathrm{Aut}\mathbf{R}$．则$\sigma|\mathbf{Q}=1$．再证对于任意 $a\in\mathbf{R}$，$a>0\iff\sigma(a)>0$．］

6. 设 $K=\mathbf{C}(x,y)$ 是复数域$\mathbf{C}$上不定元x和y 的有理分式域，$F=\mathbf{C}(x^n+y^n,xy)$．证明K/F是Galois扩张，它的Galois群$G(K/F)$是由$\sigma:(x,y)\longmapsto(y,x)$和$\tau:(x,y)\longmapsto(\zeta x,\zeta^{-1}y)$ $(\zeta=e^{2\pi i/n})$所生成的$2n$阶群（二面体群）．

7. 设K是域F上一个有限次Galois 扩域，E是K/F的一个中间域．证明，存在E的唯一的最小扩域 L，$F\subseteq E\subseteq L\subseteq K$．使得 L/F 是 Galois 张扩，并且

$$G(K/L)=\bigcap_{\sigma\in G(K/F)}\sigma G(K/E)\sigma^{-1}.$$

8. 设K是域F上一个有限次Galois扩域．L,M是K/F的中间域．证明

(i) $G(K/LM)=G(K/L)\cap G(K/M)$；

(ii) $G(K/L\cap M)=G(K/L)\vee G(K/M)$，

这里$G(K/L)\vee G(K/M)$表示$G(K/L)$与$G(K/M)$所生成的子群，即$G(K/F)$中包含$G(K/L)$及$G(K/M)$的最小的子群；

(iii) 如果$G(K/L)\cap G(K/M)=\{1\}$，可以得出什么结论？

9. 设L是域F的一个正规扩域，K是F在L中的可分闭包。证明K是F的Galois扩域。

10. 设F是一个完备域，Ω是F的一个代数闭包。证明Ω是F的Galois扩域。

3.2 一些例子

在叙述Galois理论的基本定理之前，我们先看几个例子。

例1 令F是一个特征不等于2的域，K是F的一个二次扩域。则K是F的Galois扩域。

事实上，设$\alpha\in K$但$\alpha\notin F$，那么$K=F(\alpha)$。α在F上的最小多项式是$f(X)=X^2+bX+c$。因为$\operatorname{char}F\neq 2$，所以$f'(X)=2X+b\neq 0$，$f(X)$是可分的，从而$K=F(\alpha)$是$F$上可分扩域。令$m=b^2-4c$，则$K=F(\sqrt{m})=F(\sqrt{m},-\sqrt{m})$，所以$K$是多项式$X^2-m$在$F$上的分裂域，因而是$F$上Galois扩域。

例2 令K是域F的正规扩域；K_s是F在K中的可分闭包。则K_s是F的Galois扩域。

事实上，K_s/F是可分的。我们只需证明K_s/F是正规的。设$\alpha\in K_s$。令$f(X)$是α在F上的最小多项式。由2.3.2，在$K[X]$内，$f(X)$可以分解成一次因式的乘积：

$$f(X)=\prod_{i=1}^{n}(X-\alpha_i),\ \alpha_i\in K\ (1\leqslant i\leqslant n).$$

因为α是F上可分元素，而$f(\alpha_i)=0$，所以$\alpha_i\in K_s$，$1\leqslant i\leqslant n$。这样，$f(X)$在$K_s[X]$内可以分解成一次因式的积。再由2.3.2，K_s是F的正规扩域。

例 3 设F是一个完备域；Ω是F的代数闭包．则Ω是F的可分正规扩域，从而是Galois扩域．特别当Char $F=0$或者F是有限域时，Ω是F的Galois扩域．

例 4 令$\mathbf{Q}$是有理数域．多项式X^3-2在$\mathbf{Q}[X]$中不可约，$E=\mathbf{Q}(\sqrt[3]{2})$是$\mathbf{Q}$的一个三次扩域．在复数域$\mathbf{C}$上，$X^3-2=(X-\sqrt[3]{2})(X-\zeta\sqrt[3]{2})(X-\zeta^2\sqrt[3]{2})$，$\zeta=e^{2\pi i/3}$．因此$K=\mathbf{Q}(\sqrt[3]{2},\zeta)=\mathbf{Q}(\sqrt[3]{2},\sqrt{-3})$是$X^3-2$在$\mathbf{Q}$上的分裂域，因而是$\mathbf{Q}$上一个Galois扩域．$[K:\mathbf{Q}]=6$．$[K:E]=2$，所以由例1，$K/E$是Galois扩张．然而$E=\mathbf{Q}(\sqrt[3]{2})\not\ni\zeta\sqrt[3]{2}$（$\sqrt[3]{2}$的共轭元素），所以$E/\mathbf{Q}$不是Galois扩张．

我们确定Galois群$G=G(K/\mathbf{Q})$．G的任意元素σ由K在$\mathbf{Q}$上的生成元$\sqrt[3]{2}$和ζ的像$\sigma(\sqrt[3]{2})$和$\sigma(\zeta)$完全确定．$\sigma(\sqrt[3]{2})$和$\sigma(\zeta)$可能的值是它们在$\mathbf{Q}$上的共轭元，$\sqrt[3]{2}$，$\zeta\sqrt[3]{2}$，$\zeta^2\sqrt[3]{2}=\zeta^{-1}\sqrt[3]{2}$和$\zeta$，$\zeta^{-1}=\zeta^2$．这样的共轭元素对$(\sigma(\sqrt[3]{2}),\sigma(\zeta))$共有六种可能．另一方面，由3.1.4，$|G|=[K:\mathbf{Q}]=6$．因此上述六个共轭元素对完全确定了群$G$的元素．

令$\sigma,\tau\in G$，它们分别是由元素对$(\sigma\sqrt[3]{2}),\sigma(\zeta))=(\zeta\sqrt[3]{2},\zeta)$和$(\tau(\sqrt[3]{2}),(\tau(\zeta))=(\sqrt[3]{2},\zeta^{-1})$所决定$K$的$\mathbf{Q}$-自同构，那么

$$G=\{1,\sigma,\sigma^2,\tau,\sigma\tau,\tau^2\tau\}.$$

G的元素由以下的表给出（ρ代表G的一般元素）：

ρ	$\rho(\sqrt[3]{2})$	$\rho(\zeta)$	阶
1	$\sqrt[3]{2}$	ζ	1
σ	$\zeta\sqrt[3]{2}$	ζ	3
σ^2	$\zeta^{-1}\sqrt[3]{2}$	ζ	3
τ	$\sqrt[3]{2}$	ζ^{-1}	2
$\sigma\tau$	$\zeta\sqrt[3]{2}$	ζ^{-1}	2
$\sigma^2\tau$	$\zeta^{-1}\sqrt[3]{2}$	ζ^{-1}	2

$G \cong S_3$。

例 5 令 p 是一个素数．X^4-p 是 $\mathbf{Q}[X]$ 中不可约多项式．令 $\alpha=\sqrt[4]{p}\in\mathbf{R}$．$E=\mathbf{Q}(\alpha)$ 是 $\mathbf{Q}$ 上四次扩域．$K=E(i)=\mathbf{Q}(\alpha,i)$ 是 X^4-p 在 $\mathbf{Q}$ 上的分裂域．因而 K 是 $\mathbf{Q}$ 上一个 Galois 扩域．$[K:\mathbf{Q}]=8$，$\mathbf{Q}\supsetneqq E\supsetneqq K$．$E\not\ni i\alpha$（$\alpha$ 的 $\mathbf{Q}$-共轭元），所以 $E/\mathbf{Q}$ 不是Galois扩张．

令 $G=G(K/\mathbf{Q})$．G 的任意元素 ρ 由它在 α 和 i 上的作用完全确定．$\rho(\alpha)$ 可能取的值是 $\pm\alpha,\pm i\alpha$；$\rho(i)$ 可能取的值是 $\pm i$，所以元素对 $(\rho(\alpha),\rho(i))$ 共有 8 种可能．然而由3.1.4，$|G|=8$．所以这样的八对元素恰好确定了 G 的全部元素．取 σ，$\tau\in G$，分别是由元素对 $(\sigma(\alpha),\sigma(i)),=(i\alpha,i)$ 和 $(\tau(\alpha),(\tau(i))=(\alpha,-i)$ 所确定的元素．则

$$G=\{1,\sigma,\sigma^2,\sigma^3,\tau,\sigma\tau,\sigma^2\tau,\sigma^3\tau\}.$$

G 与二面体群 D_4 同构，G 的元素由下面的表给出：

ρ	$\rho(\alpha)$	$\rho(i)$	阶
1	α	i	1
σ	$i\alpha$	i	4
σ^2	$-\alpha$	i	2
σ^3	$-i\alpha$	i	4
τ	α	$-i$	2
$\sigma\tau$	$i\alpha$	$-i$	2
$\sigma^2\tau$	$-\alpha$	$-i$	2
$\sigma^3\tau$	$-i\alpha$	$-i$	2

例 6 有限域的Galois群．

设 $F=F_q$ 是 q 元有限域，K 是 F 的一个 f 次扩域．$K=F_{q^f}$ 是可分多项式 $X^{q^f}-X\in F[X]$ 在 F 上的分裂域，因而是 F 的 Galois 扩域．

K的乘法群$K^{\times}=K\setminus\{0\}$是一个$q^f-1$阶循环群，它由一个元素$\theta\in K^{\times}$生成。

$$\sigma: K\ni\alpha\longmapsto\alpha^q\in K$$

是K的一个F-自同构，所以$\sigma\in G(K/F)$。

设σ的阶为m。那么

$\sigma^m=1\Longleftrightarrow\sigma^m(\alpha)=\alpha,\ \forall\alpha\in K\Longleftrightarrow\theta=\sigma^m(\theta)=\theta^{q^m}\Longleftrightarrow=\theta^{q^m-1}=1$。因为$\theta$的阶是$q^f-1$，而$m$是使$\sigma^m=1$的最小正整数，所以$m=f$。这样，$1,\sigma,\cdots,\sigma^{f-1}$是$G(K/F)$中互不相同的元素。然而由3.1.4，$|G(K/F)|=[K:F]=f$。所以

$$G(K/F)=\{1,\sigma,\cdots,\sigma^{f-1}\}$$

是由σ所生成的f阶循环群。

习　题

1. 设char$F\neq3$，K是域F上一个三次不可约多项式的一个分裂域。证明$G(K/F)$同构于三次对称群或三次交错群。

2. 设$K=\mathbf{Q}(\sqrt{2},i)$。试求$K/\mathbf{Q}$的Galois群及群表。

3. 设F是一个域，$K=F(\alpha)$，$\alpha^n=1$，其中n是使得等式$\alpha^n=1$成立的最小正整数。证明，K/F的Galois群是Abel群。

4. (i) 设$d\in\mathbf{Q}$，且$d\geqslant0$，$K=\mathbf{Q}(\sqrt{d})$，证明$G(K/\mathbf{Q})$或者是单位元群或者同构于$\mathbf{Z}/2\mathbf{Z}$。

(ii) 证明复数域$\boldsymbol{C}$是实数域$\boldsymbol{R}$上的Galois扩域。

5. 设$F(X)$是域F上不定元X的有理分式域，$G=\{1,\sigma,\tau\}\subset G(F(X)/F)$，其中1是恒等自同构，$\sigma$和$\tau$分别是由

$$X\longmapsto\frac{1}{1-X}\text{和}X\longmapsto\frac{X-1}{X}$$

所导出的$F(X)$的F-自同构。证明，G是$G(F(X)/F)$的子群，并且确定G的固定域$F(X)^G$。

3.3 基本定理

在这一节里，我们将叙述并且证明Galois理论的基本定理。

设K/F是一个Galois扩张，$G=G(K/F)$是它的Galois群。由3.1.1，我们有

$$F=K^G=\{a\in K|\ \sigma(a)=a,\ \forall\sigma\in G\}.$$

设H是G的一个子群。那么显然有

$$F=K^G\subseteq K^H\subseteq K.$$

即H的固定域K^H是K/F的一个中间域。反过来设E是K/F的一个中间域。由3.1.6，K/E也是Galois扩张，并且$G(K/E)$是G的一个子群。

令$\{H\}$是G的子群族（G的一切子群所组成的集），$\{E\}$是K/F的中间域族。那么

$$\Phi: H\longmapsto K^H$$

定义了$\{H\}$到$\{E\}$的一个映射，另一方面。

$$\Gamma: E\longmapsto G(K/E)$$

是$\{E\}$到$\{H\}$的一个映射。我们考虑合成映射$\Phi\circ\Gamma$和$\Gamma\circ\Phi$。因为K/E是Galois扩张，所以

$$\Phi\circ\Gamma(E)=\Phi(G(K/E))=K^{G(K/E)}=E.$$

即$\Phi\circ\Gamma$是$\{E\}$到自身的恒等映射。另一方面，映射$\Gamma\circ\Phi$不一定是$\{H\}$到自身的恒等映射(参看本节习题7)。然而这种情况只有在K是F的无限次扩域时才有可能发生。我们将证明，当K是F的有限次扩域时，$\Gamma\circ\Phi$也是恒等映射，从而在$\{H\}$与$\{E\}$之间可以建立一个双射。

先证以下的

引理 3.3.1 设K是一个域，G是K的全体自同构群$\mathrm{Aut}(K)$的一个有限子群，$F=K^G$是G的固定域。则

$$[K:F]\leqslant |G|.$$

证 设$n=|G|$．我们只需证明，K中任意$m>n$个元素都在F上线性相关．令$G=\{\sigma_1=1,\sigma_2,\cdots,\sigma_n\}$．设$\alpha_1,\alpha_2,\cdots,\alpha_m$是$K$中$m>n$个元素．那么以下的系数在$K$内$m$个未知量$x_1,x_2,\cdots,x_m$，$n$个方程的齐次线性方程组

$$(1)\qquad \sum_{j=1}^{m}\sigma_i(\alpha_j)x_j=0,\ i=1,2,\cdots,n,$$

在K中有非零解．在所有这样的非零解中，选取一个解$(b_1,b_2,\cdots,b_m)$使得所含非零分量b_j的个数最少．必要时重新对未知量编号，可设$b_1\neq 0$．又因为$b_1^{-1}(b_1,b_2,\cdots,b_m)$也是方程组的一个解，所以我们不妨假设$b_1=1$．我们证明，每一个$b_j$都在$F$内，从而方程组(1)的第一个方程($\sigma_1=1$)就是

$$\alpha_1+b_2\alpha_2+\cdots+b_m\alpha_m=0,$$

由此就得出$\alpha_1,\alpha_2,\cdots,\alpha_m$在$F$上线性相关．

如果某一个$b_j\notin F$，不失一般性可设$b_2\notin F$．由于$F=K^G$，所以有$\sigma_k\in G$，使得$\sigma_k(b_2)\neq b_2$．把σ_k作用于方程组

$$\sum_{j=1}^{m}\sigma_i(\alpha_j)b_j=0,1\leqslant i\leqslant n$$

的每一个方程，我们得到

$$\sum_{j=1}^{m}\sigma_k\sigma_i(\alpha_j)\sigma_k(\sigma_j)=0,1\leqslant i\leqslant n.$$

然而$\{\sigma_k\sigma_1,\cdots,\sigma_k\sigma_m\}=\{\sigma_1,\cdots,\sigma_m\}$，所以

$$\sum_{j=1}^{m}\sigma_i(\alpha_j)\sigma_k(b_j)=0,\ 1\leqslant i\leqslant n.$$

这就是说，$(1,\sigma_k(b_2),\cdots,\sigma_k(b_m))$也是方程组(1)的一个解．由解$(1,b_2,\cdots,b_m)$减去这个解得$(0,b_2-\sigma_k(b_2),\cdots,b_m-\sigma_k(b_m))$，它仍是(1)的非平凡解，因为$b_2-\sigma_k(b_2)\neq 0$．这个解所含非零分量的个数小于$(b_1,b_2,\cdots,b_m)$中非零分量的个数，这与$(b_1,b_2,\cdots,b_m)$的取法矛盾．这样，必须所有$b_j\in F$． ∎

定理 3.3.2 令K是一个域，G是K的全体自同构群$\mathrm{Aut}(K)$的一个子群. $F=K^G$是G的固定域. 如果G是有限群，那么K是F的有限次 Galois扩域，并且G就是扩张K/F的 Galois群.

证 如果$|G|<\infty$，那么由 3.3.1，$[K:F]\leqslant|G|$，所以K是F的有限次 Galois 扩域. 由3.1.4，我们有$|G(K/F)|=$ $=[K:F]$. 注意到$G\subseteq G(K/F)$，于是$G=G(K/F)$. ∎

现在我们来陈述和证明 Galois 理论的基本定理.

定理 3.3.3 (Galois 理论的基本定理) 设K是域F的一个有限次 Galois 扩域. $G=G(K/F)$是K/F的Galois 群. 对于G的每一个子群H，令H的固定域$E=K^H$与它对应，那么$\Phi: H\longmapsto E$是G的子群族与K/F的中间域族之间的一个双射.

证 设E是K/F的一个中间域，我们已经看到.

$$\Gamma: E\longmapsto G(K/E)$$

是K/F的中间域族$\{E\}$到G的子族$\{H\}$的一个映射，并且对于任意中间域E，$\Phi\circ\Gamma(E)=E$. 只剩下证明，$\Gamma\circ\Phi$是G的子群族$\{H\}$的恒等映射.

因为K/F是有限次 Galois 扩张，所以G是有限群，设H是G的任意一个子群. 令$E=\Phi(H)=K^H$是H的固定域. 由3.3.2，$H=G(K/E)=\Gamma(\Phi(H))$，这就是说. $\Gamma\circ\Phi$是G的子群族$\{H\}$的恒等映射. 因而Φ是双射. ∎

我们以下用$H\longleftrightarrow E$表示子群族$\{H\}$与中间域族$\{H\}$的如上定义的双射. 关于这个双射的细节，有以下

定理 3.3.4 设K是域F的一个有限次 Galois 扩域. G是K/F的Galois 群. 在3.3.3 中所定义的G的子群族$\{E\}$与K/F的中间域族$\{E\}$之间的双射满足以下条件：

(i) $G\longleftrightarrow F$; $\{1\}\longleftrightarrow K$.

(ii) 设$H\longleftrightarrow E$，则$[K:E]=|H|$, $[E:F]=(G:H)$,

这里$(G:H)$表示子群H对于G的指数。

(iii) $H_i \longleftrightarrow E_i$，$i=1,2$，$H_1 \subseteq H_2 \Longleftrightarrow E_1 \supseteq E_2$。

(iv) $H \longleftrightarrow E$，$\sigma \in G$，则$\sigma H \sigma^{-1} \longleftrightarrow \sigma(E)$。

(v) $H_i \longleftrightarrow E_i$，$i=1,2$，则$H_1$与$H_2$在$G$中共轭$\Longleftrightarrow E_1$与$E_2$在$F$上共轭。

(vi) $H \longleftrightarrow E$，H是G的正规子群$\Longleftrightarrow E$是F的Galois扩域；在这个情况下$G(E/F) \cong G/H$。

证 (i) 是显然的。

(ii) 因为$H=G(K/E)$，由3. 1. 4，$[K:E]=|H|$。于是

$$[E:F]=[K:F]/[K:E]=|G|/|H|=(G:H).$$

(iii) 显然。

(iv) 令$E'=\sigma(E)$。设$\tau \in \mathrm{Aut}(K)$。那么

$$\begin{aligned}\tau \in G(K/E') &\Longleftrightarrow \tau(\beta)=\beta, \quad \forall \beta \in E'=\sigma(E)\\ &\Longleftrightarrow \tau\sigma((\alpha)=\sigma(\alpha), \quad \forall \alpha \in E\\ &\Longleftrightarrow \sigma^{-1}\tau\sigma(\alpha)=\alpha, \quad \forall \alpha \in E\\ &\Longleftrightarrow \sigma^{-1}\tau\sigma \in H\\ &\Longleftrightarrow \tau \in \sigma H \sigma^{-1},\end{aligned}$$

所以 $G(K/E')=\sigma H \sigma^{-1}$。

(v) 设存在$\sigma \in G$使得$\sigma H_1 \sigma^{-1}=H_2$。由(iv)就有$\sigma(E_1)=E_2$。反之，设$E_1, E_2$在$F$上共轭。因为$K/F$是Galois扩张，所以$E_1$到$E_2$的$F$-共轭可以开拓为$K$的一个$F$-自同构，即存在$\sigma \in G=G(K/F)$使得$\sigma(E_1)=E_2$。由(iv)，$\sigma H_1 \sigma^{-1}=H_2$。

(iv) 设H是G的正规子群。那么

$$\sigma H \sigma^{-1}=H, \quad \forall \sigma \in G.$$

由(iv)，

$$\sigma(E)=E, \quad \forall \sigma \in G.$$

令$\sigma'=\sigma|_E$。则$\sigma' \in G(E/F)$。映射

$$f: G \ni \sigma \longmapsto \sigma' \in G(E/F)$$
是群G到群$G(E/F)$的同态映射．设$\sigma' \in G(E/F)$．因为K/F是正规扩张，所以σ'可以开拓为G的一个元素σ，即存在$\sigma \in G$，使得$\sigma|_E = \sigma'$．所以f是满同态．

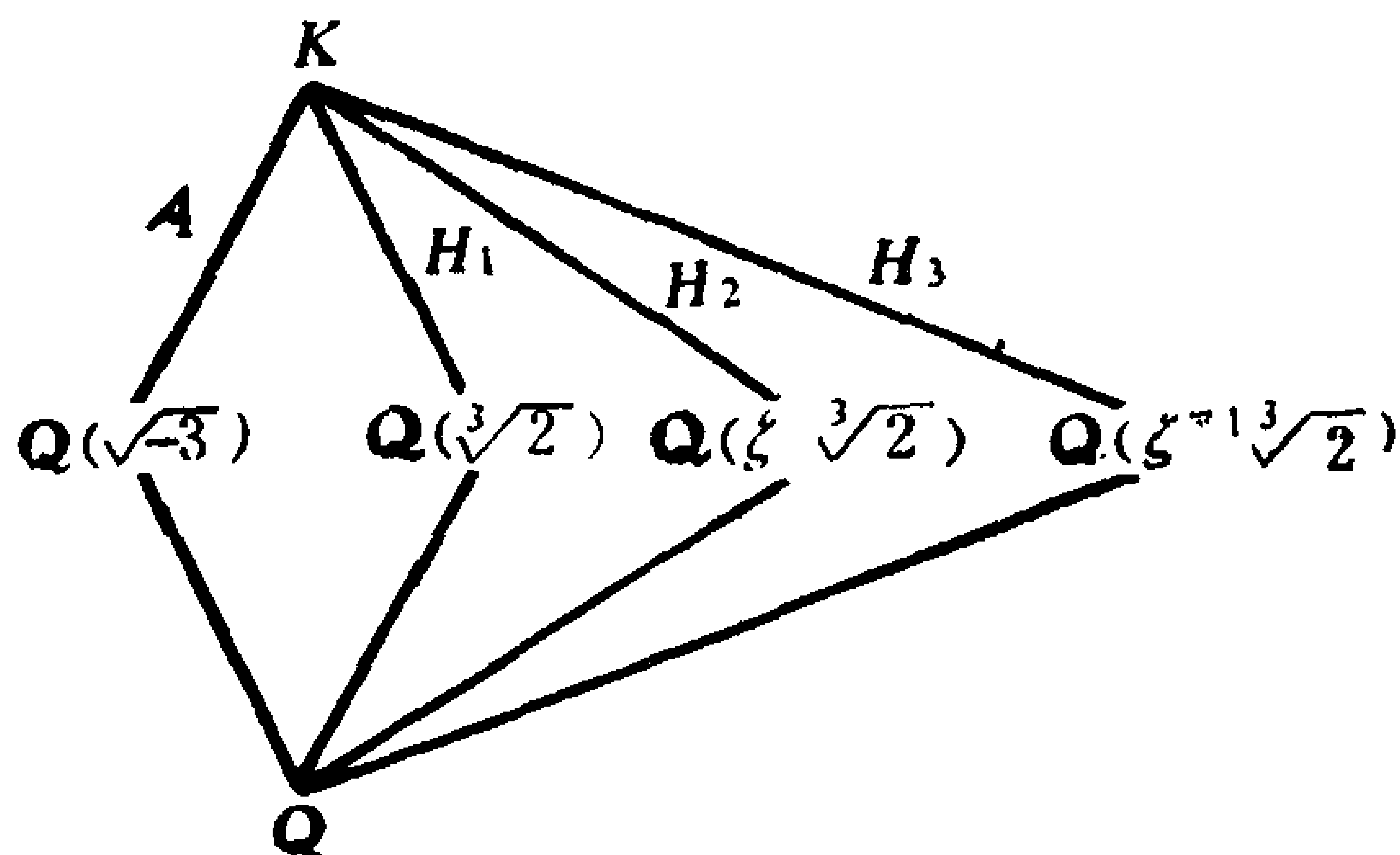
$$\mathrm{Ker}(f) = \{\sigma \in G \mid \sigma(\alpha) = \alpha,\ \forall \alpha \in E\} = G(K/E) = H.$$
所以$G(E/F) \cong G/H$．

由(ii)．$[E:F] = (G:H) = |G(E/F)|$，由 3.1.4，E/F是Galois扩张．

反之，如果E/F是Galois扩张，那么E/F是正规扩张，所以$\sigma(E) = E$，$\forall \sigma \in G$．由(iv)，$\sigma H \sigma^{-1} = H$，$\forall \sigma \in G \Longrightarrow H$是正规子群． ▮

例 1 $K = \mathbf{Q}(\sqrt{-3}, \sqrt[3]{2})$是有理数域$\mathbf{Q}$上 6 次 Galois 扩域．$K/\mathbf{Q}$的 Galois 群$G = G(K/\mathbf{Q})$由
$$\sigma: (\sqrt{-3}, \sqrt[3]{2}) \longmapsto (\sqrt{-3}, \zeta\sqrt[3]{2})$$
$$\tau: (\sqrt{-3}, \sqrt[3]{2}) \longmapsto (-\sqrt{-3}, \sqrt[3]{2})$$
生成，这里$\zeta = e^{2\pi i/3}$，$G \cong S_3$（参看§3.2，例4）．
$$G = \{1, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\},$$
$$\sigma^3 = 1, \tau^2 = 1, \sigma\tau = \tau\sigma^2$$

G共有四个真子群：



$A=\{1,\sigma,\sigma^2\}$

$H_1=\{1,\tau\}, H_2=\{1,\sigma^2\tau\}, H_3=\{1,\sigma\tau\}$.

其中A是正规子群。我们有

$$\sigma H_1\sigma^{-1}=H_2, \sigma^2 H_1\sigma^{-2}=H_3.$$

所以H_1, H_2, H_3是两两共轭的子群。

K/Q的中间域与G的子群之间的对应关系见84页的图。

例2 $K=Q(\sqrt[4]{3}, i)$, $i=\sqrt{-1}$，是有理数域Q上8次Galois扩域。K/Q的Galois群G是由

$$\sigma: (\sqrt[4]{3}, i)\longmapsto(i\sqrt[4]{3}, i),$$

$$\tau: (\sqrt[4]{3}, i)\longmapsto(\sqrt[4]{3}, -i)$$

所生成的8阶二面体群（参看3.2，例5）。

$$G=\{1,\sigma,\alpha^2,\sigma^3,\tau,\sigma\tau,\sigma^2\tau,\sigma^3\tau\}.$$

$$\sigma^4=1, \tau^2=1, \sigma\tau=\tau\sigma^3.$$

G的真子群计有

五个二阶子群：

$H_1=\{1,\sigma^2\}$; $H_2=\{1,\sigma^3\tau\}$; $H_3=\{1,\sigma\tau\}$;

$H_4=\{1,\sigma^2\tau\}$; $H_5=\{1,\tau\}$.

三个四阶子群（正规子群）：

$J_1=\{1,\sigma,\sigma^2,\sigma^3\}$;

$J_2=\{1,\sigma^2,\tau,\sigma^2\tau\}=H_1\times H_5=H_1\times H_4=H_4\times H_5$;

$J_3=\{1,\sigma^2,\sigma^3\tau,\sigma\tau\}=H_1\times H_2=H_1\times H_3=H_2\times H_3$.

H_1是正规子群，$\sigma H_2\sigma^{-1}=H_3, \sigma H_5\sigma^{-1}=H_4$.

令 $E_i=\Phi(H_i)=K^{H_i}, i=1,2,3,4,5$

$L_i=\Phi(J_i)=K^{J_i}, i=1,2,3.$

则

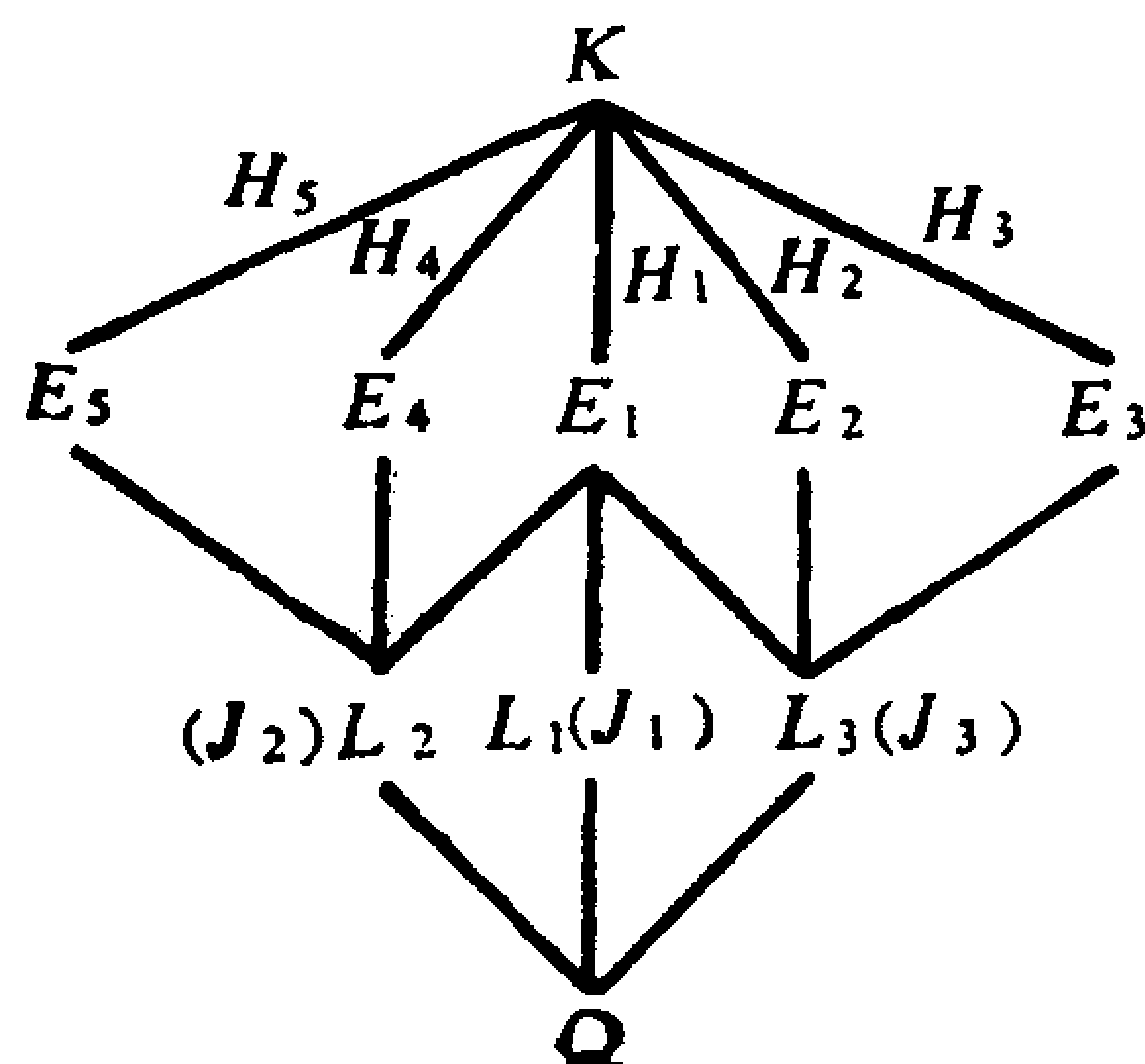
$E_1=Q(\sqrt{3}, i), E_2=Q((1-i)\sqrt[4]{3})$,

$E_3=Q((1+i)\sqrt[4]{3})$,

$E_4=Q(i\sqrt[4]{3}), E_5=Q(\sqrt[4]{3})$.

$L_1=\mathbf{Q}(i), L_2=\mathbf{Q}(\sqrt{3}), L_3=\mathbf{Q}(i\sqrt{3})$.

它们的关系由下图表示：



习 题

1. 设$K=\mathbf{Q}(\sqrt{2},\sqrt{3})$. 则$K/\mathbf{Q}$是Galois扩张（3.1，习题1）. 写出Galois群G（$K/\mathbf{Q}$）的子群与$K/\mathbf{Q}$的中间域之间的对应关系。

2. 设K/F是一个有限次Galois扩张，$G=G(K/F)$是它的Galois群，且G可以写成它的子群H_1与H_2的直积：$G=H_1\times H_2$。令$K_i=K^{H_i}$，$i=1,2$，证明，$K=K_1K_2$。

3. 设$K=\mathbf{Q}(\sqrt{2},\sqrt{-3},\sqrt[3]{5})$.

（i） 证明$K/\mathbf{Q}$是Galois扩张.

（ii） 决定Galois群$G(K/\mathbf{Q})$.

（iii） 求出$G(K/\mathbf{Q})$的所有子群及$K/\mathbf{Q}$的所有中间域.

4. 设K_1和K_2都是域F的有限次Galois扩域，并且都包含在F的某一个扩域内。

（i） 证明，K_1K_2是F的Galois扩域.

（ii） 令

$H=\{(\sigma_1,\sigma_2)|\ \sigma_i\in G(K_i/F), i=1,2,$ 且 $\sigma_1|_{K_1\cap K_2}=$
$=\sigma_2|_{K_1\cap K_2}\}$。证明，$H$ 是直积 $G(K_1/F)\times G(K_2/F)$ 的子群，且

$$G(K_1K_2/F)\cong H.$$

(iii) 如果 $K_1\cap K_2=F$，则

$$G(K_1K_2/F)\cong G(K_1/F)\times G(K_2/F).$$

5. 设 $f(X)$ 是域 F 上一个多项式，K 是 $f(X)$ 在 F 上一个分裂域。在 $K[X]$ 内，

$$f(X)=(X-\alpha_1)^{k_1}\cdots(X-\alpha_s)^{k_s}.$$

$\alpha_i\in K$，且互不相同，$k_i>0$ $(1\leqslant i\leqslant s)$。令

$$g(X)=(X-\alpha_1)\cdots(X-\alpha_s)$$

又令 $u_0,u_1,\cdots,u_s\in K$ 是 $g(X)$ 的系数，$E=F(u_0,u_1,\cdots,u_s)$。证明 K/E 是 Galois 扩张，且 $G(K/E)\cong G(K/F)$。

6. 设 $E=\mathbf{Q}(\sqrt{2},\sqrt{3})$，

$$\alpha=\sqrt{\sqrt{6}(\sqrt{2}+\sqrt{3})(1+\sqrt{2})},\qquad K=E(\alpha).$$

(i) 证明，$E/\mathbf{Q}$ 是四次 Galois 扩张，且 $G(E/\mathbf{Q})$ 与 Klein 四元群同构。

(ii) 设 $G(E/\mathbf{Q})=\{1_E,\sigma,\tau,\rho\}$。算出 $\rho(\alpha^2)$，$\sigma(\alpha^2)$ 和 $\tau(\alpha^2)$。

(iii) 设 $\tilde{\varepsilon},\tilde{\rho},\tilde{\sigma},\tilde{\tau}$ 是 K 的 $\mathbf{Q}$-共轭，满足条件：$\tilde{\varepsilon}|_E=1_E$，$\tilde{\sigma}|_E=\sigma$，$\tilde{\tau}|_E=\tau$，$\tilde{\rho}|_E=\rho$。计算 $\tilde{\varepsilon}(\alpha)$，$\tilde{\rho}(\alpha)$，$\tilde{\sigma}(\alpha)$ 和 $\tilde{\tau}(\alpha)$。

(iv) 证明 $\alpha\notin E$，从而 $K/\mathbf{Q}$ 是八次 Galois 扩张。

(v) 证明，$G(K/\mathbf{Q})$ 由 $\tilde{\sigma}$ 和 $\tilde{\tau}$ 生成，并且满足关系

$$\tilde{\sigma}^4=1,\ \tilde{\tau}^{-1}\tilde{\sigma}\tilde{\tau}=\tilde{\sigma}^{-1},\ \tilde{\tau}^2=\tilde{\sigma}^2.$$

从而 $G(K/\mathbf{Q})$ 与四元数群 Q_8 同构。

(vi) 找出 $G(K/\mathbf{Q})$ 的一切子群与 $K/\mathbf{Q}$ 的一切中间域之间的对应关系。

7. 令 $F=F_p$ 是一个 p 元有限域，p 是一个素数，Ω 是 F 的

一个代数闭包。则。取定一个整数$l>2$。令F_i表示F上Ω中唯一的l^i次扩域$F_{q_i}, q_i=p^i$。

$$F=F_0\subset F_1\subset F_2\subset\cdots\subset\Omega.$$

令$N=\bigcup_{i\geqslant 0}F_i$.

（i） 证明，N是F的Galois扩域.

(ii) 令$\varphi: N\ni\alpha\longmapsto\alpha^p\in N$。证明$\varphi$是$N$的一个$F$-自同构，从而$\varphi$属于$N/F$的Galois群$G(N/F)$。

(iii) 令$G=G(N/F)$。设

$$H=\{\varphi^n\mid n\in\mathbf{Z}\}$$

是G中由φ所生成的循环子群．证明：

(a) $\Phi(H)=\Phi(G)=F$;

(b) $G\neq H$.

从而对于Galois扩张N/F来说，$\Gamma\circ\Phi$不是G的子群族的恒等映射。

［提示］ 要证明(b)成立，可令

$$l_i=1+l+\cdots+l^{i-1}=(1-l^i)/(1-l), i\geqslant 1.$$

对于任意$\alpha\in N$，则$\alpha\in F_i$，对于某个i．定义$\sigma(\alpha)=\varphi^{l_i}(\alpha)$。证明$\sigma$的定义不依赖于$i$，因而$\sigma(\alpha)$是由$\alpha$唯一确定的，并且$\sigma\in G$，但$\sigma\notin H$。

3.4 单位根

为了以下的讨论，在这一节里，先作一些准备工作。

设F是一个域。$F^\times$是F的一切非零元素所构成的乘法群。n是一个正整数.$\zeta\in F$叫做一个n次单位根，如果$\zeta^n=1$。

F中一个n次单位根ζ叫做一个**本原n次单位根**，如果对于任意小于n的正整数m来说，$\zeta^m\neq 1$。

设$\zeta\in F$。如果ζ是某一个n次单位根，那么就称ζ是一个

单位根。

令W_F表示F中一切单位根的集。则W_F是$F^\times$的一个子群。令W_n表示F中一切n次单位根所成的集。则W_n是W_F的一个有限子群。

定理 3.4.1 (i) W_n是有限循环群；W_n的阶$|W_n|$整除n。

(ii) $|W_n|=n \Longleftrightarrow F$含有本原$n$次单位根。

在这个情况下，F所含本原n次单位根的个数等于$\varphi(n)$，这里$\varphi(n)$表示 Euler 函数，即小于n且与n互素的正整数的个数。

(iii) 设F含有本原n_i次单位根，$1\leqslant i\leqslant s$，令n是$n_1,\cdots,n_s$的最小公倍。则F含有本原n次单位根。

(iv) 设$\mathrm{char}F=p>0$。如果F含有本原n次单位根，则$p\nmid n$。

(v) 设F是一个代数闭域。如果$\mathrm{char}F=0$，则对于任意n，F含有本原n次单位根；如果$\mathrm{char}F=p>0$，则对于任意不被p整除的n，F含有本原n次单位根。

证 (i) W_n是$F^\times$的有限子群，而$F^\times$的有限子群是循环群(2.4.8)，所以W_n是循环群。令ζ是W_n的一个生成元，m是ζ的阶。则$m=|W_n|$。因为$\zeta^n=1$，所以$m|n$，即$|W_n|\,|n$。

(ii) $|W_n|=n \Longleftrightarrow W_n$的生成元$\zeta$的阶为$n \Longleftrightarrow \zeta$是$F$中一个本原$n$次单位根。

再者，$\zeta\in F$是一个本原n次单位根$\Longleftrightarrow \zeta$是$W_n$的生成元。因此，$F$所含的本原$n$次单位根的个数等于$W_n$的生成元的个数，而后者显然等于$\varphi(n)$。

(iii) 设$\zeta_i\in F$是一个本原的n_i次单位根$1\leqslant i\leqslant s$。n是$n_1,\cdots,n_s$的最小公倍。则$\zeta_i^n=1$，从而$\zeta_i\in W_n$。所以ζ_i的阶n_i整除$|W_n|$，$1\leqslant i\leqslant s$。因此$n\,|\,|W_n|$。另一方面，由(i)，$|W_n|\,|n$。

这样一来就有$|W_n|=n$。再由(ii)，F含有一个本原n次单位根。

(iv) 设$\zeta\in F$是一个本原n次单位根。如果$p|n$，则$(\zeta^{n/p})^p=1\Longrightarrow(\zeta^{n/p}-1)^p=0\Longrightarrow\zeta^{n/p}=1$。而$n/p<n$，这与$\zeta$是本原$n$次单位根的假设相违。

(v) 设 $f(X)=X^n-1\in F[X]$。$f'(X)=nX^{n-1}$。在$\mathrm{char}F=0$或$\mathrm{char}F=p>0$，而$p\nmid n$的情况下，$f'(X)\neq 0$。所以$f(X)$与$f'(X)$互素，因而$f(X)$没有重根。因为F是代数闭域，所以$f(X)$在F中有n个互不相同的根，从而$|W_n|=n$。所以F含有本原n次单位根。 ▮

现在我们定义分圆多项式的概念。

设Ω是一个代数闭域。如果$\mathrm{char}\,\Omega=0$，我们取n是任意正整数；如果$\mathrm{char}\,\Omega=p>0$，我们就取$n$是任意一个不能被$p$整除的正整数。由上面的定理可知$\Omega$含有$\varphi(n)$个本原$n$次单位根。令$P_n$是$\Omega$中一切本原$n$次单位根所成的集。$\Omega[X]$的多项式

$$\Phi_n(X)=\prod_{\eta\in P_n}(X-\eta)$$

叫做一个**分圆多项式**。

显然，$\deg\Phi_n(X)=\varphi(n)$。取定一个本原n次单位根η。那么

$$\Phi_n(X)=\prod_{\substack{a\leqslant n\\(a,n)=1}}(X-\eta^a).$$

令$W_n=\{\zeta\in\Omega\,|\,\zeta^n=1\}$是一切$n$次单位根所成的集。由3.4.1(ii)，$W_n$是一个$n$阶循环群。设$\zeta\in W_n$。那么

ζ是一个d阶元素$(d|n)\Longleftrightarrow\zeta$是一个本原$d$次单位根

$\Longleftrightarrow\zeta$是$\Phi_d(X)$的根。

因此我们有

(1)
$$X^n-1=\prod_{\substack{d|n\\1\leqslant d\leqslant n}}\Phi_d(X).$$

定理 3.4.2 设Ω是一个代数闭域。

（i） 如果 $\mathrm{char}\,\Omega=0$，则 $\Phi_n(X)$是一个最高次项系数是 1 的 $\varphi(n)$次整系数多项式：$\Phi_n(X)\in \mathbf{Z}[X]$。

（ii） 如果 $\mathrm{char}\,\Omega=p>0$，则 $\Phi_n(X)$是F_p上一个最高次项系数是 1 的 $\varphi(n)$次多项式：$\Phi_n(X)\in F_p[X]$。

证 对 n 作归纳法。

设 $\mathrm{char}\,F=0$。当 $n=1$ 时，$\Phi_1(X)=X-1\in \mathbf{Z}[X]$ 且最高次项系数是 1。

设$n>1$，我们有

$$X^n-1=\Phi_n(X)\prod_{\substack{d\mid n\\ 1\leqslant d<n}}\Phi_d(X).$$

由归纳法假设，$\prod_{\substack{d\mid n\\ 1\leqslant d<n}}\Phi_d(X)$ 是最高次项系数为 1 的整系数多项式，因而是本原多项式，于是由本原多项式的性质，

$$\Phi_n(X)\in \mathbf{Z}[X].$$

对于 $\mathrm{char}\,\Omega=p>0$ 的情形，同样可以对 n 用归纳法来证明。 ∎

现在设 $\Omega=C$是复数域。则$\Phi_n(X)\in \mathbf{Z}[X]$。在$C$中，全体 n 次单位根是

$$W_n=\{e^{2k\pi i/n}\mid k=0,1,\cdots,n-1\}.$$

当且仅当 $(k,n)=1$ 时，$e^{2k\pi\sqrt{-1}/n}$ 是本原 n 次单位根。所以在 $C[X]$里，分圆多项式是

$$\Phi_n(X)=\prod_{\substack{1\leqslant a\leqslant n\\ (a,n)=1}}(X-e^{2a\pi\sqrt{-1}/n})$$

定理 3.4.3 分圆多项式$\Phi_n(X)$在$Q[X]$中不可约。

证 因为 $\Phi_n(X)\in \mathbf{Z}[X]$，所以只要证明，$\Phi_n(X)$ 不能分解成两个次数都低于$\varphi(n)$的整系数多项式的乘积。假设 $f(X)\in \mathbf{Z}[X]$是$\Phi_n(X)$的一个不可约因式。不妨设 $f(X)$的最高次项系

数是1．由(1)，存在$g(X)\in \mathbf{Z}[X]$使得$X^n-1=f(X)g(X)$．我们证明，$f(X)$满足以下条件：

(*) 设p是一个素数且$p\nmid n$．如果$f(\zeta)=0$，则$f(\zeta^p)=0$．

事实上，设$f(\zeta^p)\neq 0$．因为在$\mathbf{Z}[X]$里，

$$X^n-1=f(X)g(X).$$

而$\zeta^n-1=f(\zeta)g(\zeta)=0$，所以

$$f(\zeta^p)g(\zeta^p)=(\zeta^p)^n-1=0,$$

从而$g(\zeta^p)=0$．以所ζ是多项式$g(X^p)\in \mathbf{Z}[X]$的根．另一方面，$f(X)$也是$\mathbf{Q}[X]$中最高次项系数是1的不可约多项式，所以$f(X)$是ζ在$\mathbf{Q}$上的最小多项式．因此，在$\mathbf{Q}[X]$里，$f(X)\mid g(X^p)$，从而在$\mathbf{Z}[X]$里，$f(X)\mid g(X^p)$．于是存在$h(X)\in \mathbf{Z}[X]$，使得

$$g(X^p)=f(X)h(X)$$

然而自然同态

$$\mathbf{Z}\in u\longmapsto \bar{u}\in \mathbf{Z}/(p)=\boldsymbol{F}_p$$

可以开拓为多项式环的同态

$$\mathbf{Z}[X]\ni f(X)=\sum a_iX^i\longmapsto h(X)=\sum \bar{a}_iX^i\in \boldsymbol{F}_p[X].$$

因为在$\mathbf{Z}[X]$里，

$$X^n-1=f(X)g(X),\quad g(X^p)=f(X)h(X),$$

所以在$\boldsymbol{F}_p[X]$里，

$$X^n-1=\overline{f}(X)\overline{g}(X),\quad \overline{g}(X^p)=\overline{f}(X)\overline{f}(X).$$

$\bar{f}(X)\in \boldsymbol{F}_p[X]$，且$\deg(\overline{f}(X))=\deg(f(X))>0$．设$\bar{u}(X)$是$\bar{f}(X)$在$\boldsymbol{F}_p[X]$内一个不可约因式．因为在$\boldsymbol{F}_p[X]$内，

$$\overline{g}(X^p)=\overline{g}(X)^p,$$

而$\overline{f}(X)\mid\overline{f}(X)^p$，所以，$\overline{u}(X)\mid\overline{g}(X)^p$．又因为$\overline{u}(X)$不可约，所以$\overline{u}(X)\mid\overline{g}(X)$．注意到$X^n-1=\overline{f}(X)\overline{g}(X)$，所以$\overline{u}(X)^2\mid(X^n-1)$，从而$X^n-1$有重根．所以$(X^n-1)'=nX^{n-1}=\mathbf{0}$．这样，必须$p\mid n$．这就导致矛盾．因此(*)成立．

现在设m是任意一个与n互素的正整数。设$m=\prod p_i$是m的素因子分解。那么对于每一个i，$p_i \nmid n$。设ζ是$f(X)$的一个根。因为$f(X)|\Phi_n(X)$，所以ζ是一个本原n次单位根。由(*)，我们有$f(\zeta^{p_1})=0$。再由(*)，$f(\zeta^{p_1p_2})=f((\zeta^{p_1})^{p_2})=0$。如此继续下去，最后得$f(\zeta^m)=0$。因为$(m,n)=1$，所以$\zeta^m$也是一个本原$n$次单位根。这样一来，所有的本原$n$次单位根都是$f(X)$的根，从而$\Phi_n(X)|f(X)$，于是$f(X)=\Phi_n(X)$，这就证明了$\Phi_n(X)$的不可约性。 ▮

推论 3.4.4 设$\zeta\in C$是一个本原n次单位根。那么ζ在Q上的最小多项式是分圆多项式$\Phi_n(X)$。$Q(\zeta)$是多项式X^n-1在Q上的分裂域；$[Q(\zeta):Q]=\varphi(n)$。 ▮

利用Möbius函数，可以得到分圆多项式的一个很有用的表达式。在这一节的最后，我们介绍一下Möbius函数的概念。

设n是一个正整数。令

$$n=p_1p_2\cdots p_\lambda$$

是n的素因子分解。我们定义

$$\mu(n)=\begin{cases}0, \text{如果存在} i\neq j \text{而} p_i=p_j; \\ (-1)^\lambda, \text{如果} p_1, p_2, \cdots, p_\lambda \text{两两不同}; \\ 1, \text{如果} n=1.\end{cases}$$

μ称为**Möbius函数**。

引理 3.4.5 当$n\geqslant 2$时，

$$\sum_{\substack{d|n \\ 1\leqslant d\leqslant n}} \mu(d)=0,$$

这里$\sum$表示对n的一切正因子求和。

证 设

$$n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$$

是n的素因子幂分解，$p_1, p_2, \cdots, p_r$是互不相同的素数，$e_i>0$，$1\leqslant i\leqslant r$。我们有

$$\sum_{d\mid n}\mu(d)=\sum\ \mu(p_1^{a_1}p_2^{a_2}\cdots p_r^{a_r}).$$

右端 $\sum$ 表示对于满足条件 $0\leqslant a_i\leqslant e_i(1\leqslant i\leqslant r)$的一切序列$(a_1, a_2,\cdots,a_r)$求和。去掉右端的和里等于零的那些项，我们有

$$\begin{aligned}\sum_{d\mid n}\mu(d)&=\mu(1)+(\mu(p_1)+\mu(p_2)+\cdots+\mu(p_r))+\\&\quad+(\mu(p_1p_2)+\cdots+\mu(p_{r-1}p_r))+\cdots+\\&\quad+\mu(p_1p_2\cdots p_r)\\&=1-r+\binom{r}{2}\cdots+(-1)^r=(1-1)^r=0.\end{aligned}$$ ▮

利用Möbius 函数，可以将分圆多项式写成比较便于计算的形式。

定理 3.4.6

$$\Phi_n(X)=\prod_{\substack{d\mid n\\1\leqslant d\leqslant n}}(X^d-1)^{\mu(n/d)}.$$

证 利用(1)，在右边的积里，以

$$X^d-1=\prod_{\substack{\delta\mid d\\1\leqslant\delta\leqslant d}}\Phi_\delta(X)$$

代入得

$$\prod_{\substack{d\mid n\\1\leqslant d\leqslant n}}(X^d-1)^{\mu(n/d)}=\prod_{\substack{d\mid n\\1\leqslant d\leqslant n}}\Big(\prod_{\substack{\delta\mid d\\1\leqslant\delta\leqslant d}}\Phi_\delta(X)\Big)^{\mu(n/d)}$$

在右端双重积里，固定每一个 δ，$\delta\mid d, d\mid n$，则n/δ 的每一个因子 δ' 都有 n/d 的形状；反之，如果 $d\mid n$ 且 $\delta\mid d$，那么 $n/d\mid n/\delta$，于是上式右端的双重积可以重新组合成以下形式：

$$\prod_{\substack{\delta\mid n\\1\leqslant\delta\leqslant n}}\Phi_\delta(X)^{\sum_{\delta'\mid(n/\delta)}\mu(\delta')}$$

因为

$$\sum_{\delta'\mid(n/\delta)}\mu(\delta')=\begin{cases}1,\text{若}n/\delta=1,\\0,\text{若}n/\delta>1.\end{cases}$$

所以

$$\prod_{\substack{d \mid n \\ 1 \leqslant d \leqslant n}} (X^d - 1)^{\mu(n/d)} = \Phi_n(X).$$ ▮

例 根据上面的表达式，容易写出。

$\Phi_1(X) = X - 1$; $\Phi_2(X) = X + 1$; $\Phi_3(X) = X^2 + X + 1$;

$\Phi_4(X) = X^2 + 1$; $\Phi_6(X) = X^2 - X + 1$; $\Phi_8(X) = X^4 + 1$.

设 p 是一个素数，那么对于任意正整数，我们有

$$\Phi_{p^\nu}(X) = (X^{p^\nu} - 1)(X^{p^{\nu-1}} - 1)^{-1}$$
$$= X^{p^{\nu-1}(p-1)} + X^{p^{\nu-1}(p-2)} + \cdots + X^{p^{\nu-1}} + 1.$$

习　　题

1. 设 n 是一个奇数。证明，多项式 $X^n - 1$ 在 F 上的分裂域也是 $X^{2n} - 1$ 在 F 上的分裂域。

2. 设 K 是一个特征为 $p > 0$ 的域。证明，K 内的一个 $p^e m$ 次单位根总是一个 m 次单位根。

3. 证明，$\mathbf{Q}$ 的有限次扩域内只含有限个单位根。

4. 证明关于 Euler 函数 φ 的下列性质：

(i) 如果 p 是一个素数，n 是一个正整数，则 $\varphi(p^n) = p^n(1 - \frac{1}{p})$；

(ii) 如果 $(m, n) = 1$，则 $\varphi(mn) = \varphi(m)\varphi(n)$；

(iii) 如果 $n = p_1^{k_1} \cdots p_1^{k_r}$，其中 p_i 是两两不同的素数，$k_i > 0\ (1 \leqslant i \leqslant r)$，则

$$\varphi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_r}).$$

(iv) $\sum_{\substack{0 < d \leqslant n \\ d \mid n}} \varphi(d) = n$；

(v) 令 d 和 l 分别是 m 和 n 的最大公因数和最小公倍数，则 $\varphi(m)\varphi(n) = \varphi(d)\varphi(l)$。

5. 设φ是 Euler 函数。

(i) 证明，若$n>2$，则$\varphi(n)$是偶数。

(ii) 找出所有满足$\varphi(n)=2$的正整数。

(iii) 找出所有满足$\varphi(n)=n/p$的正整数对(n,p)，其中p是一个素数。

6. 证明关于**Q**上分圆多项式$\Phi_n(X)$的下列性质：

(i) $\Phi_p(X)=\Phi_{p^k}(X^{p^{k-1}})$，$p$是一个素数，$k>0$。

(ii) 设 $n=p_1^{k_1}\cdots p_r^{k_r}$（$p_i$是两两不同的素数，$k_i>0$，$1\leqslant i\leqslant r$）。则

$$\Phi_n(X)=\Phi_{p_1\cdots p_r}(X^{p_1^{k_1-1}\cdots p_r^{k_r-1}}).$$

(iii) 如n是奇数，则$\deg\Phi_{2n}(X)=\deg\Phi_n(X)$。

(iv) 设p是一个素数且$p\nmid n$，则

$$\Phi_{pn}(X)=\Phi_n(X^p)/\Phi_n(X).$$

(v) 若$n=p^k$，p是素数，$k>0$，则$\Phi_n(1)=p$；在其它情形，$\Phi_n(1)=0$。

7. 写出$\Phi_{12}(X)$和$\Phi_{36}(X)$的表达式。

3.5 分圆扩域

设K是域F的一个 Galois 扩域，如果 Galois 群$G(K/F)$是一个 Abel 群，那么就称K是F的一个 **Abel 扩域**（K/F称为**Abel 扩张**）.

一类重要的 Abel 扩张就是所谓的分圆扩张。

设F是一个域。Ω是F的代数闭包。Ω/F的一个中间域K叫做F的一个**分圆扩域**，如果K是通过对F添加某些单位根而生成的。

根据这个定义，如果K是F的一个分圆扩域，那么$K=F(W_K)$，这里W_K是K所含的一切单位根所成的集。

定理 3.5.1 域F的分圆扩域是 Abel 扩域。

证 设K是域F的一个分圆扩域．首先证明，K是F的Galois扩域．令W_K是K所含的单位根的全体．设$\zeta\in W_K$，$\zeta\neq 1$．令n是ζ的阶．则$\zeta^n=1$，而对于任意$1\leqslant m\leqslant n$，$\zeta^m\neq 1$．所以$\mathrm{char}F\nmid n$．因此X^n-1是$F[X]$的一个可分多项式．所以ζ是F上可分元素．这样，$K=F(W_K)$是F的可分扩域．

再来证明K是F的正规扩域．设K'是一个与K在F上共轭的域．那么存在K与K'的一个共同的扩域M和K到K'的一个F-同构σ．我们有$K=F(W_K)$，$K'=F(\sigma(W_K))$，这里

$$\sigma(W_K)=\{\sigma(\zeta)\mid\zeta\in W_K\}.$$

因为σ是K到K'的同构映射，所以$\sigma(W_K)$恰是K'所含的单位根的全体$W_{K'}$．于是$K'=F(W_{K'})$．设$\zeta\in W_K$是W_K的一个n阶元素．则$\zeta^n=1$．从而$\sigma(\zeta)^n=1$．所以$\sigma(\zeta)\in W_{K'}$．这样，$\sigma(\zeta)$也是一个n次单位根．然而$1,\zeta,\cdots,\zeta^{n-1}\in M$是全部$n$次单位根，所以必有某一个$i$，$0\leqslant i\leqslant n-1$，使得$\sigma(\zeta)=\zeta^i$．所以$\sigma(\zeta)\in W_K$，从而$W_{K'}=\sigma(W_K)\subseteq W_K$．以$\sigma^{-1}$代$\sigma$，我们同样地可以得出．$W_K\subseteq W_{K'}$．这样．$W_K=W_{K'}$而$K=K'$．所以$K$是$F$的Galois扩域．

以上证明了K/F是Galois扩张．

现在证明K/F是Abel扩张．设$\sigma,\tau\in G(K/F)$．由以上的证明可知，对于任意$\zeta\in W_K$，存在整数i和j，使得$\sigma(\zeta)=\zeta^i$，$\tau(\zeta)=\zeta^j$．于是

$$\sigma\tau(\zeta)=\zeta^{ij}=\tau\sigma(\zeta).$$

由于$K=F(W_K)$．所以对于K的任意元素α都有$\sigma\tau(\alpha)=\tau\sigma(\alpha)$．所以$\sigma\tau=\tau\sigma$，即$G(K/F)$是Abel群． ∎

定理 3.5.2 设K是域F的一个扩域．对于K来说，以下两个条件是等价的：

（i） K是F的有限次分圆扩域；

（ii） 存在一个本原单位根$\zeta\in K$，使得$K=F(\zeta)$．

证 (i)$\Longrightarrow$(ii) $K=F(W_K)$。因为$[K:F]<\infty$，所以总可以选取有限个$\zeta_1,\cdots,\zeta_s\in W_K$，使得$K=F(\zeta_1,\cdots,\zeta_s)$，这里$\zeta_i$是一个本原$n_i$次单位根，$1\leqslant i\leqslant s$。令$n$是$n_1,\cdots,n_s$的最小公倍。由3.4.1，$W_K$含有一个本原$n$次单位根$\zeta$；而$\zeta_i=\zeta^{m_i}$，这里$m_i$是某一个正整数，$1\leqslant i\leqslant s$。于是

$$K=F(\zeta_1,\cdots,\zeta_s)\subseteq F(\zeta)\subseteq F(W_K)\subseteq K,$$

所以$K=F(\zeta)$。

(ii)$\Longrightarrow$(i) $K=F(\zeta)$是分圆扩域，且$[K:F]<\infty$。 ▌

设n是一个正整数。令$\bar{a}=a \bmod n$是整数a关于以n为模的剩余类。我们知道，

$$\{\bar{a}\mid a\in \mathbf{Z},\ (a,n)=1\}$$

作成剩余类环$\mathbf{Z}/(n)$的一个乘法群，称为**以n为模的不可约剩余类群**，记作$(\mathbf{Z}/(n))^*$。

定理 3.5.3 设n不能被域F的特征整除，ζ是一个本原n次单位根。那么分圆扩域$K=F(\zeta)$的Galois群$G(K/F)$与$(\mathbf{Z}/(n))^*$的一个子群同构。

证 $\zeta\in K$是一个本原n次单位根，因此K含有全体n次单位根所成的n阶循环群W_n，ζ是W_n的一个生成元。设$\sigma\in G(K/F)$。则$\sigma(\zeta)\in W_n$也是一个本原n次单位根，所以

$$\sigma(\zeta)=\zeta^{\nu(\sigma)}.$$

这里$\nu(\sigma)$是一个与n互素的整数。如果m是一个整数，使得$\sigma(\zeta)=\zeta^m$，则

$$m\equiv\nu(\sigma) \mod n.$$

设$\sigma,\tau\in G(K/F)$，那么

$$\zeta^{\nu(\sigma\tau)}=\sigma\tau(\zeta)=\zeta^{\nu(\sigma)\nu(\tau)}.$$

因此

$$\nu(\sigma\tau)\equiv\nu(\sigma)\nu(\tau) \mod n.$$

这样，

$$\nu: G(K/F) \ni \sigma \longmapsto \overline{\nu(\sigma)} \in (\mathbf{Z}/(n))^*$$

是群 $G(K/F)$ 到群 $(\mathbf{Z}/(n))^*$ 内的同态映射. 如果

$$\nu(\sigma) \equiv 1 \mod n.$$

则 $\sigma(\zeta)=\zeta$; 从而 $\sigma=1$, 所以 ν 是单射. 这就是说, $G(K/F)$ 与 $(\mathbf{Z}/(n))^*$ 的一个子群同构. ▌

设 F 是一个域, n 是一个正整数且 $\mathrm{char}F \nmid n$. 我们知道, 在 F 的一个代数闭包 Ω 内的全体 n 次单位根作成一个 n 阶循环群 W_n. $K=F(W_n)$ 是多项式 X^n-1 在 F 上的分裂域. 我们有 $K=F(\zeta)$, ζ 是一个本原 n 次单位根. 由上面所证的定理, K/F 是一个 Galois 扩张而群 $G(K/F)$ 与 $(\mathbf{Z}/(n))^*$ 的一个子群同构. 这个同构是这样建立的:

$$\nu: G(K/F) \ni \sigma \longmapsto \overline{\nu(\sigma)} \in (\mathbf{Z}/(n))^*,$$

这里 $\sigma(\zeta)=\zeta^{\nu(\sigma)}$. 剩余类 $\overline{\nu(\sigma)}$ 不依赖于 W_n 的生成元 ζ 的选取. 事实上, 设 ζ' 也是一个本原 n 次单位根. 那么 $K=F(\zeta')$. 我们有 $\zeta'=\zeta^a$, 这里 a 是一个与 n 互素的整数. 设 $\sigma(\zeta')= =\zeta'^{\nu'(\sigma)}$. 于是

$$\zeta'^{\nu'(\sigma)}=\sigma(\zeta')=\sigma(\zeta^a)=\sigma(\zeta)^a$$
$$=\zeta^{a\nu(\sigma)}=\zeta'^{\nu(\sigma)}.$$

所以

$$\nu'(\sigma) \equiv \nu(\sigma) \mod n.$$

这样, 我们就证明了以下的

推论 3.5.4 设 F 是一个域, n 是一个正整数且 $\mathrm{char}F \nmid n$. 多项式 X^n-1 在 F 上的分裂域 K 是一个 Abel 扩域. Galois 群 $G(K/F)$ 与 $(\mathbf{Z}/(n))^*$ 的一个子群同构. ▌

例 1 令 $W=\{e^{2k\pi i/n} \mid n=1, 2, \cdots; 0 \leqslant k \leqslant n-1\}$ 是复数域 $\mathbf{C}$ 内一切单位根所成的集. $\mathbf{C}$ 的子域 $\mathbf{Q}(W)$ 是 $\mathbf{Q}$ 的一个无限次的 Abel 扩域.

例 2　令$F=F_q$是q元有限域．$m\geqslant 2$是一个正整数且$(m,q)=1$．ζ是一个本原m次单位根（含于F的某一个扩域内）．设$K=F(\zeta)$．则$W_K=K$．

$$[K:F]=[F_q(\zeta):F_q]=f,$$

这里f是满足

$$q^f\equiv 1 \bmod m$$

的最小正指数．它是群$(\mathbf{Z}/(m))^*$中q所在的剩余类$\overline{q}$的阶．因此$G(K/F)$与$(\mathbf{Z}/(m))^*$中由$\overline{q}$所生成的子群$\langle\overline{q}\rangle$同构．

最后，利用前一节有关的结果，我们有

定理 3.5.5　对有理数域$\mathbf{Q}$添加一个本原n次单位根ζ所得的分圆扩域$K=\mathbf{Q}(\zeta)$是$\mathbf{Q}$的一个$\varphi(n)$次 Abel 扩域，这里$\varphi(n)$表示 Euler 函数．Galois 群$G(K/\mathbf{Q})$由一切

$$\sigma_a:\zeta\longmapsto\zeta^a,\ (a,n)=1,$$

组成，它与以n为模的不可约剩余类群$(\mathbf{Z}/(n))^*$同构．

证　定理的前一个断言是3.5.2和3.4.4的直接结果．只剩下证明后一个断言．由3.5.3，

$$\nu: G(K/\mathbf{Q})\ni\sigma\longmapsto\overline{\nu(\sigma)}\in(\mathbf{Z}/(n))^*$$

是一个群同态单射，这里$\sigma(\zeta)=\zeta^{\nu(\sigma)}$．另一方面，$|G(K/\mathbf{Q})|=[K:\mathbf{Q}]=\varphi(n)=|(\mathbf{Z}/(n))^*|$．所以$\nu$是满射．∎

为了确定而见，我们把对有理数域$\mathbf{Q}$添加一个本原n次单位根ζ所得的分圆扩域$\mathbf{Q}(\zeta)$叫做**圆的n分域**．

习　题

1. (i)　设p是一个奇素数．证明，不可约剩余类群$(\mathbf{Z}/(p^n))^*$是一个阶为$p^{n-1}(p-1)$的循环群．

(ii)　当$p=2, n=1$或2时，(i)也成立．

(iii)　当$n\geqslant 3$时，不可约剩余类群$(\mathbf{Z}/(2^n))^*$是一个二阶循环子群与一个2^{n-1}阶循环子群的直积．

2. 设K/F是有限次 Galois 扩张．G是它的 Galois 群，H是G的一个子群，E是与H对应的K/F的中间域．证明，E/F是 Abel扩张当且仅当$H\supseteq[G,G]$，这里$[G,G]$表示G的换位子群．

3. 设K_1，K_2都是域F的某一个代数闭包Ω的子域，且$K_i\supseteq\supseteq F$都是Abel 扩域，$i=1,2$．证明，K_1K_2也是F的 Abel 扩域．

4. 设m，n是两个正整数，d和l分别是m，n的最大公约数和最小公倍数．令K_m和K_n分别表示圆的m分域和n分域．证明，$K_m\cap K_n$是圆的d分域，K_mK_n是圆的l分域．

5. 令$K_n=\mathbf{Q}(\zeta)$是圆的n分域，ζ是一个本原n次单位根．

(i) 设p是一个奇素数．问$[K_{p^r}:\mathbf{Q}]=?$

(ii) $K_2=\mathbf{Q}$，$K_4=\mathbf{Q}(\sqrt{-1})$．

(iii) 当$r\geqslant 3$时，$K_{2^r}=\mathbf{Q}(\sqrt{-1})\mathbf{Q}(\cos(\pi/2^{r-1}))$．且$\mathbf{Q}(\sqrt{-1})\cap\mathbf{Q}(\cos(\pi/2^{r-1})=\mathbf{Q}$．

6. 记号同第5题．

(i) 确定$K_5/\mathbf{Q}$的所有中间域；

(ii) 确定$K_8/\mathbf{Q}$的所有中间域；

(iii) 确定$K_7/\mathbf{Q}$的所有中间域．设ζ是一个本原7次单位根，求$\zeta+\zeta^{-1}$在$\mathbf{Q}$上的最小多项式．

7. 设$n>2$，ζ是一个本原n次单位根．则$[\mathbf{Q}(\zeta+\zeta^{-1}):\mathbf{Q}]=\varphi(n)/2$．

3.6 范和迹

我们以下将讨论另一类重要的Abel扩张，这种扩张的Galois群是循环群，为此，在这一节里，先介绍范和迹的概念，这两个概念本身也是重要的．

设K是域F的一个有限次扩域，Ω是F的一个包含K的代数闭包。令$\sigma_1,\cdots,\sigma_m$是K到Ω内的一切互不相同的F-共轭。对于$\alpha\in K$，定义

$$N_F^K(\alpha)=\left(\prod_{j=1}^{m}\sigma_j(\alpha)\right)^{[K:F]_i},$$

称为α的范。定义

$$T_F^K(\alpha)=[K:F]_i\sum_{j=1}^{m}\sigma_j(\alpha),$$

称为α的迹。

下面我们即将看到，范和迹都是域F的元素（见3.6.2），因而不依赖于代数闭包Ω的选取。当K/F是可分扩张时，$[K:F]_i=1$，在不致引起混淆的情况下，我们这时将N_F^K和T_F^K分别简写作N和T：

$$N(\alpha)=\prod_{j=1}^{m}\sigma_j(\alpha);\quad T(\alpha)=\sum_{j=1}^{m}\sigma_j(\alpha).$$

例1 设$K=\mathbf{C}$，$F=\mathbf{R}$，$\Omega=\mathbf{C}$。那么K到$\mathbf{C}$内的$\mathbf{R}$-共轭只有两个。即$\mathbf{C}$的恒等自同构1_C和对合$\sigma: a+b\sqrt{-1}\longmapsto a-b\sqrt{-1}\ (a,b\in\mathbf{R})$。于是

$$N(a+bi)=(a+bi)(a-bi)=a^2+b^2;$$
$$T(a+bi)=(a+bi)+(a-bi)=2a.$$

例2 设$\operatorname{char}F=p>0$，$K=F(\alpha)$是一个n次单扩域，$f(X)$是α在F上的最小多项式，Ω是K的一个代数闭包，m是$f(X)$的可分次数，p^e是$f(X)$的不可分次数。那么在$\Omega[X]$内，

$$f(X)=(X-\alpha_1)^{p^e}\cdots(X-\alpha_m)^{p^e},$$

$\alpha_1,\cdots,\alpha_m$两两不同，$\alpha=\alpha_1$。于是

$$N_F^K(\alpha)=\left(\prod_{j=1}^{m}\alpha_j\right)^{p^e};$$

$$T_F^K(\alpha) = {}^{pe} \cdot \sum_{j=1}^{m} \alpha_j.$$

特别，如果 α 是可分元素，则$T_F^K(\alpha)$就是$f(X)$中X^{n-1}的系数改变符号。$N_F^K(\alpha)$就是 $f(X)$的常数项乘以$(-1)^n$。

定理 3.6.1 设K是域F的一个有限次Galois扩域，$G(K/F)=\{\sigma_1,\cdots,\sigma_m\}$，那么对于任意$\alpha\in K$，

$$N_F^K(\alpha) = \prod_{j=1}^{m} \sigma_j(\alpha);$$

$$T_F^K(\alpha) = \sum_{j=1}^{m} \sigma_j(\alpha).$$

证 取定K的一个代数闭包Ω。因为K/F是Galois扩张，所以$\sigma_1,\cdots,\sigma_m$就是K到Ω内的全部F-共轭。又因为K/F是可分的，所以$[K:F]_i=1$。 ▮

定理 3.6.2 设K是域F的一个有限次扩域。$\alpha,\beta\in K$。

(i) $N_F^K(\alpha\beta)=N_F^K(\alpha)N_F^K(\beta)$; $T_F^K(\alpha+\beta)=T_F^K(\alpha)+$ $+T_F^K(\beta)$。

(ii) 如果 $\alpha\in F$，则

$$N_F^K(\alpha)=\alpha^{[K:F]};\quad T_F^K(\alpha)=[K:F]\alpha.$$

(iii) 设 $f(X)=X^n+a_1X^{n-1}+\cdots+a_n\in F[X]$是$\alpha$在$F$上的最小多项式。则

$$N_F^K(\alpha)=((-1)^n a_n)^{[K:F(\alpha)]};$$

$$T_F^K(\alpha)=-[K:F(\alpha)]a_1.$$

因此，$N_F^K(\alpha)$，$T_F^K(\alpha)\in F$。

(iv) 设E是K/F的一个中间域。则

$$N_F^E(N_E^K(\alpha))=N_F^K(\alpha);\quad T_F^E(T_E^K(\alpha))=T_F^K(\alpha).$$

(由(iii), $N_E^K(\alpha),T_E^K(\alpha)\in E$)。

证 (i) 直接由定义得出。

(ii) 因为$[K:F]=[K:F]_s[K:F]_i$，再根据 2.8.5，

即可得出(ii)。

(iii) 令$E=F(\alpha)$。$F\subseteq E\subseteq K$。取定F的一个包含K的代数闭包。设$\{\sigma_1,\cdots,\sigma_m\}$是一切$E$到$\Omega$内的$F$-共轭，$\{\tau_1,\cdots,\tau_l\}$是一切$K$到$\Omega$内的$E$-共轭。由2.6.1，

$$\{\sigma_k\tau_j \mid 1\leqslant k\leqslant m,\ 1\leqslant j\leqslant l\}$$

是一切K到Ω内的F-共轭。由2.8.5，$[K:E]_s=l$，而

$$[K:E]=[K:E]_s[K:E]_i=l[K:E]_i.$$

又由2.8.6，$[K:F]_i=[K:E]_i[E:F]_i$。因为$\alpha\in E$，所以

$$N_F^K(\alpha)=\left(\prod_{k=1}^{m}\prod_{j=1}^{l}\sigma_k\tau_j(\alpha)\right)^{[K:F]_i}$$

$$=\left(\prod_{k=1}^{m}\sigma_k(\alpha)^l\right)^{[K:F]_i}$$

$$=\left(\prod_{k=1}^{m}\sigma_k(\alpha)\right)^{l[K:E]_i[E:F]_i}$$

$$=\left(\prod_{k=1}^{m}\sigma_k(\alpha)\right)^{[K:E][E:F]_i}.$$

同样地，

$$T_F^K(\alpha)=[K:E][E:F]_i\sum_{k=1}^{m}\sigma_k(\alpha).$$

因为$\sigma_i: E=F(\alpha)\to F(\sigma_i(\alpha))$是$E$到$\Omega$内的$F$-共轭，由2.2.7，$\sigma_1(\alpha),\cdots,\sigma_m(\alpha)$恰是$f(X)$的一切互不相同的根。所以

$$f(X)=\left(\prod_{k=1}^{m}(X-\sigma_k(\alpha))\right)^{[E:F]_i}$$

$$=\left(X^m-\sum_{k=1}^{m}\sigma_k(\alpha)X^{m-1}+\cdots+\right.$$

$$\left.+(-1)^m\prod_{k=1}^{m}\sigma_k(\alpha)\right)^{[E:F]_i}$$

如果$[E:F]_i=1$，则$m=n$，这时(iii)成立。设$[E:F]_i=$

$=p^f>1$，$p=\text{char } F$，$f>0$。那么

$$a_n=(-1)^{mp^f}\left(\prod_{k=1}^{m}\sigma_k(\alpha)\right)^{p^f}=(-1)^n\left(\prod_{k=1}^{m}\sigma_k(\alpha)\right)^{p^f}$$

而

$$N_F^K(\alpha)=\left(\prod_{k=1}^{m}\sigma_k(\alpha)\right)^{p^f[K:E]}=\left((-1)^n a_n\right)^{[K:E]}.$$

在这个情况下，$a_1=0$，而

$$T_F^K(\alpha)=p^f[K:E]\sum_{k=1}^{m}\sigma_k(\alpha)=0,$$

所以(iii)成立。

(iv) 记号同(iii)。我们有

$$N_E^K(\alpha)=\left(\prod_{j=1}^{l}\tau_j(\alpha)\right)^{[K:E]_i}\in E.$$

于是

$$N_F^E(N_E^K(\alpha))=N_F^E\left(\left(\prod_{j=1}^{l}\tau_j(\alpha)\right)^{[K:E]_i}\right)$$

$$=\left(N_F^E\left(\prod_{j=1}^{l}\tau_j(\alpha)\right)\right)^{[K:E]_i}$$

$$=\left(\prod_{k=1}^{m}\prod_{j=1}^{l}\sigma_k\tau_j(\alpha)\right)^{[E:F]_i[K:E]_i}$$

$$=\left(\prod_{k=1}^{m}\prod_{j=1}^{l}\sigma_k\tau_j(\alpha)\right)^{[K:F]_i}=N_F^K(\alpha).$$

另一方面，

$$T_E^K(\alpha)=[K:E]_i\sum_{j=1}^{l}\tau_j(\alpha)\in E.$$

所以

$$T_F^E(T_E^K(\alpha))=[K:E]_i[E:F]_i\sum_{k=1}^{m}\sigma_k\left(\sum_{j=1}^{l}\tau_j(\alpha)\right)$$

$$=[K:F]_i \sum_{k=1}^{m} \sum_{j=1}^{l} \sigma_k \tau_j(\alpha) = T_F^K(\alpha). \qquad \blacksquare$$

习　　题

1. 证明，在范和迹的定义里，取F的一个包含K的正规扩域N来代替Ω，这样定义的范和迹与原来的定义是等价的。并且这个定义不依赖于N的选取。

2. 设$F=F_q$是一个q元有限域，K是F的一个有限次扩域。证明：

$$N: K \ni \alpha \longmapsto N_F^K(\alpha) \in F,$$

$$T: K \ni \alpha \longmapsto T_F^K(\alpha) \in F$$

都是K到F的满射。

3. 设K是域F上一个有限次可分扩域。对于任意$\alpha, \beta \in K$，定义

$$B(x, y) = T(\alpha\beta).$$

证明，$B: K \times K \to F$是一个非退化对称双线性函数。

4. 设K是域F上一个n次可分扩域。证明，K中n个元素$\alpha_1, \alpha_2, \cdots, \alpha_n$构成$K$在$F$上一个基必要且只要$n \times n$矩阵$(B(\alpha_i, \alpha_j))_{i,j=1}^n$非退化，这里$B$是第三题所定义的双线性函数。

5. 设K/F是一个n次可分扩张，$\alpha_1, \cdots, \alpha_n$是$K$在$F$上一个基。行列式$\det(B(\alpha_i, \alpha_j))$叫做$K/F$的**判别式**。这里$B(\alpha_i, \alpha_j) = T(\alpha_i\alpha_j)$，$i, j = 1, 2, \cdots, n$。

(i) 证明。如果$\beta_1, \cdots, \beta_n$也是K在F上一个基，则$\det(B(\beta_i, \beta_j)) = c^2 \det(B(\alpha_i, \alpha_j))$，这里$c$是$F$中一个非零元素。

(ii) 设$K=F(\alpha)$是单扩域。对于基$1, \alpha, \cdots, \alpha^{n-1}$，计算$K/F$的判别式。

3.7 循环扩域

设F是一个域，K是F的一个Galois扩域。如果Galois群$G(K/F)$是一个循环群，那么就称K是F的一个**循环扩域**，相应地，K/F称为**循环扩张**。

关于循环扩张的信息是清楚的。我们先做一点准备工作。

引理 3.7.1 设K是一个域，S是K的一些自同构所组成的集。则S在K上线性无关。

证 如果存在 $\sigma_1,\cdots,\sigma_m\in S$ 和K中不全为零的元素 $a_1,\cdots,a_m$，使得对于任意 $\alpha\in K$ 来说，都有

(1) $$a_1\sigma_1(\alpha)+\cdots+a_m\sigma_m(\alpha)=0.$$

可设m是S中满足这样线性关系的元素的最小个数。显然 $m>1$。因为$\sigma_1\neq\sigma_2$，所以存在$\beta\in K$，使得$\sigma_1(\beta)\neq\sigma_2(\beta)$。对于任意$\alpha\in K$，我们有

$$a_1\sigma_1(\alpha)\sigma_1(\beta)+a_2\sigma_2(\alpha)\sigma_2(\beta)+\cdots+a_m\sigma_m(\alpha)\sigma_m(\beta)$$
$$=a_1\sigma_1(\alpha\beta)+a_2\sigma_2(\alpha\beta)+\cdots+a_m\sigma_m(\alpha\beta)=0.$$

另一方面，用$\sigma_1(\beta)$乘(1)式得

$$a_1\sigma_1(\alpha)\sigma_1(\beta)+a_2\sigma_2(\alpha)\sigma_1(\beta)+\cdots$$
$$+a_m\sigma_m(\alpha)\sigma_1(\beta)=0.$$

把这两个式子相减得

$$a_2(\sigma_2(\beta)-\sigma_1(\beta))\sigma_2(\alpha)+\cdots$$
$$+a_m(\sigma_m(\beta)-\sigma_1(\beta))\sigma_m(\alpha)=0.$$

因为$a_2\neq0$，$\sigma_2(\beta)-\sigma_1(\beta)\neq0$，这样一来就得到$S$中元素的一个更短的线性关系。与$m$的最小性矛盾。 ∎

引理 3.7.2 设K是域F的一个n次循环扩域，σ是Galois群$G(K/F)$的一个生成元。对于K中的元素α，

(i) $T_F^K(\alpha)=0\Longleftrightarrow$存在$\beta\in K$使得$\alpha=\beta-\sigma(\beta)$。

(ii) $N_F^K(\alpha)=1\Longleftrightarrow$存在$\beta\in K$，$\beta\neq0$使得$\alpha=\beta\sigma(\beta)^{-1}$。

证 $G(K/F)=\{1=\sigma^n,\sigma,\cdots,\sigma^{n-1}\}$。我们有

$$T(\alpha)=T_F^K(\alpha)=\alpha+\sigma(\alpha)+\cdots+\sigma^{n-1}(\alpha),$$
$$N(\alpha)=N_F^K(\alpha)=\alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha).$$

(i) 如果存在 $\beta\in K$，使得 $\alpha=\beta-\sigma(\beta)$，则

$$T(\alpha)=T(\beta-\sigma(\beta))=\beta+\sigma(\beta)+\cdots+\sigma^{n-1}(\beta)$$
$$-\sigma(\beta)-\cdots-\sigma^{n-1}(\beta)-\sigma^n(\beta)=0.$$

反之，设 $T(\alpha)=0$。我们可以如下地选取$\gamma\in K$，使得$T(\gamma)=1$：首先，由3.7.1，$1,\sigma,\cdots,\sigma^{n-1}$ 在K上线性无关，所以 $1+\sigma+\cdots+\sigma^{n-1}\neq 0$。因此存在 $\delta\in K$，使得

$$T(\delta)=\delta+\sigma(\delta)+\cdots+\sigma^{n-1}(\delta)\neq 0.$$

由3.6.2(iii)，$T(\delta)\in F$，所以$T(\delta)^{-1}\in F$。从而$\sigma(T(\delta)^{-1}\delta)=T(\delta)^{-1}\sigma(\delta)$。取$\gamma=T(\delta)^{-1}\delta\in K$。那么

$$T(\gamma)=T(\delta)^{-1}\delta+T(\delta)^{-1}\sigma(\delta)+\cdots+T(\delta)^{-1}\sigma^{n-1}(\delta)$$
$$=T(\delta)^{-1}T(\delta)=1.$$

现在取

$$\beta=\alpha\gamma+(\alpha+\sigma(\alpha))\sigma(\gamma)+(\alpha+\sigma(\alpha)+\sigma^2(\alpha))\sigma^2(\gamma)+\cdots$$
$$+(\alpha+\sigma(\alpha)+\cdots+\sigma^{n-2}(\alpha))\sigma^{n-2}(\gamma).$$

则

$$\sigma(\beta)=\sigma(\alpha)\sigma(\gamma)+(\sigma(\alpha)+\sigma^2(\alpha))\sigma^2(\gamma)+(\sigma(\alpha)+$$
$$+\sigma^2(\alpha)+\sigma^3(\alpha))\sigma^3(\gamma)+\cdots+$$
$$+(\sigma(\alpha)+\sigma^2(\alpha)+\cdots+\sigma^{n-1}(\alpha))\sigma^{n-1}(\gamma).$$

因为$T(\alpha)=0$，所以 $\sigma(\alpha)+\cdots+\sigma^{n-1}(\alpha)=-\alpha$。于是

$$\beta-\sigma(\beta)=\alpha\gamma+\alpha\sigma(\gamma)+\alpha\sigma^2(\gamma)+\cdots+$$
$$+\alpha\sigma^{n-2}(\gamma)+\alpha\sigma^{n-1}(\gamma)$$
$$=\alpha(\gamma+\sigma(\gamma)+\cdots+\sigma^{n-1}(\gamma))=\alpha T(\gamma)=\alpha.$$

(ii) 如果 $\alpha=\beta\sigma(\beta)^{-1}$，那么 $\sigma^j(\alpha)=\sigma^j(\beta)\sigma^{j+1}(\beta)^{-1}$，而$\sigma^n(\beta)^{-1}=\beta^{-1}$，所以

$$N(\alpha)=\prod_{j=0}^{n-1}\sigma^{j}(\alpha)=\prod_{j=0}^{n-1}\sigma^{j}(\beta)\sigma^{j+1}(\beta)^{-1}=\beta\beta^{-1}=1.$$

反之，设$N(\alpha)=1$，则 $\alpha\neq 0$. 因为 $1,\sigma,\cdots,\sigma^{n-1}$ 线性无关，所以存在 $\eta\in K$，使得

$$\beta=\alpha\eta+\alpha\sigma(\alpha)\sigma(\eta)+\alpha\sigma(\alpha)\sigma^2(\alpha)\sigma^2(\eta)+\cdots$$
$$+\alpha\sigma(\alpha)+\cdots\sigma^{n-1}(\alpha)\sigma^{n-1}(\eta)\neq 0.$$

又 $\alpha\sigma(\alpha)\cdots\sigma^{n-1}(\alpha)\sigma^{n-1}(\eta)=N(\alpha)\sigma^{n-1}(\eta)=\sigma^{n-1}(\eta)$. 所以

$$\alpha^{-1}\beta=\eta+\sigma(\alpha)\sigma(\eta)+\cdots+\sigma(\alpha)\cdots\sigma^{n-2}(\alpha)\sigma^{n-2}(\eta)+$$
$$+\sigma(\alpha)\cdots\sigma^{n-1}(\alpha)\sigma^{n-1}(\eta)=\sigma(\beta).$$

所以 $\alpha=\beta\sigma(\beta)^{-1}$. ∎

现在我们来研究有限次循环扩域的构造. 先证明

定理 3.7.3 设F是一个域且 char $F=p>0$，K是 F 的一个 n 次循环扩域. 如果 $n=mp^f,(m,p)=1,f\geqslant 0$，那么存在一串中间域

$$K\supseteq E_0\supseteq E_1\supseteq\cdots\supseteq E_f=F,$$

其中K是E_0的一个m次循环扩域，而 E_{i-1}是E_i的一个 p 次循环扩域，$1\leqslant i\leqslant f$（若 $f>0$）.

证 因为 $G=G(K/F)$是循环群，所以G的每一个子群都是正规的；又因为G的每一个子群和每一个同态像都是循环群，所以对于 K/F 的每一个中间域E来说，K/E和 E/F 都是循环扩张. 由此容易推出，对于 K/F 的任意两个中间域L，M，如果 $F\subseteq L\subseteq M\subseteq K$，则 M/L 是循环扩张.

G有唯一的m阶循环子群H. 令$E_0=\Phi(H)$是H的固定域，则$H=G(K/E_0)$，K是E_0的一个m次循环扩域，而E_0是F的一个 p^f 次循环扩域. 因为 $G(E_0/F)$ 是一个 p^f 阶循环群，所以有一个正规子群链，

$$\{e\}=G_0\lhd G_1\lhd\cdots\lhd G_{f-1}\lhd G_f=G(E_0/F),$$

这里$|G_i|=p^i$，$(G_i:G_{i-1})=p$，$i=1,\cdots,f$. 令

$$E_i=\{\alpha\in E_0\mid\sigma(\alpha)=\alpha,\ \forall\sigma\in G_i\}$$

是 G_i 的固定域。由基本定理，我们有

(a) $E_0\supseteq E_1\supseteq\cdots\supseteq E_{f-1}\supseteq E_f=F$；

(b) $[E_{i-1}:E_i]=(G_i:G_{i-1})=p$；

(c) $G(E_{i-1}/E_i)\cong G_i/G_{i-1}$。

所以 E_{i-1} 是 E_i 的一个 p 次循环扩域，$i=1,\cdots,f$。 ▮

由于这个定理，对于一个 n 次循环扩域的讨论可以归结为以下两个情形：

情形 1 $n=\mathrm{char}\,F=p>0$。

情形 2 $\mathrm{char}\,F=0$ 或 $\mathrm{char}F=p>0$ 但 $(p,n)=1$。

在情形 1，循环扩域的结构由以下定理完全解决。

定理 3.7.4 设 $\mathrm{char}F=p>0$。K 是 F 的一个 p 次循环扩域当且仅当 K 是 F 上一个形如 X^p-X-a 的不可约多项式的分裂域，这时 $K=F(\alpha)$，α 是 X^p-X-a 的任意一个根。

证 设 K/F 是 p 次循环扩张，$G=G(K/F)$ 是一个 p 阶循环群。令 σ 是 G 的一个生成元。由 3.6.2 (ii)，$T_F^K(1)=[K:F]\cdot 1=p\cdot 1=0$。于是由 3.7.2 (i)，存在 $\beta\in K$，使得 $\beta-\sigma(\beta)=1$。令 $\alpha=-\beta$。则 $\sigma(\alpha)=\alpha+1\neq\alpha$。所以 $\alpha\notin F$。因为 $[K:F]=p$，所以 K/F 没有真中间域。因此必须 $K=F(\alpha)$。然而 $\sigma(\alpha^p)==\sigma(\alpha)^p=\alpha^p+1$，所以 $\sigma(\alpha^p-\alpha)=\alpha^p-\alpha$。所以 $a=\alpha^p-\alpha\in F$。这样，α 是 F 上多项式 $f(X)=X^p-X-a$ 的一个根。因为 $\deg(f(X))=p=[K:F]$，所以 $f(X)$ 在 $F[X]$ 中不可约。

令 $j\in F_p$，F_p 是 F 的素域。则 $j^p=j$。于是

$$(\alpha+j)^p-(\alpha+j)-a=\alpha^p-\alpha-a=0.$$

所以 $\alpha+j\in K$ 也是 $f(X)$ 的根，$j=0,1,\cdots,p-1$。如果 $i,j\in F_p$，$i\neq j$，则 $\alpha+i\neq\alpha+j$。这样一来。$\alpha+j$，$j=0,1,\cdots,p-1$ 恰是 $f(X)$ 的全部根，它们都属于 K，因此，$K=F(\alpha)$ 是 $f(X)$ 在 F 上的分裂域。

最后，显然 $F(\alpha)=F(\alpha+j)$，$j=0,1,\cdots,p-1$。

反过来，设K是$f(X)=X^p-X-a\in F[X]$在F上的分裂域。我们先不要求$f(X)$在$F[X]$中不可约。设$\alpha\in K$是$f(X)$的一个根。由上一段的证明，我们看到，$F(\alpha)$包含$f(X)$的全部根$\alpha+j$，$j=0,1,\cdots,p-1$，这些根两两不同。所以$K=F(\alpha)$是F的可分正规扩域，因而是Galois扩域。$G=G(K/F)$的每一个元素τ由它在α上的作用完全确定。$\tau(\alpha)=\alpha+j$对某一个$j\in F_p$，如果$\tau,\tau'\in G$，$\tau(\alpha)=\alpha+j$，$\tau'(\alpha)=\alpha+j'$，那么$\tau\tau'(\alpha)=\alpha+j+j'$。因此，

$$\theta: G\ni\tau\longmapsto j\in F_p,\quad 若\ \tau(\alpha)=\alpha+j,$$

是群G到以p为模的剩余类加群$F_p=\mathbf{Z}/(p)$的一个同态单射。于是$G\cong\mathrm{Im}\theta\subseteq\mathbf{Z}/(p)$。因为$p$是一个素数，所以$\mathrm{Im}\theta=\{1\}$或$\mathrm{Im}\theta=\mathbf{Z}/(p)$。如果是前者，则$G=\{1\}$而$[K:F]=1$，从而$\alpha\in F$。这时$f(X)$在$F[X]$内已经完全分解成线性因式的乘积。这样，如果$f(X)$在$F[X]$中不可约，必须$G\cong\mathbf{Z}/(p)$，这时$G$是一个$p$阶循环群。 ▮

推论 3.7.5 设F是一个特征为$p>0$的域。那么多项式$f(X)=X^p-X-a\in F[X]$或者不可约，或者在$F[X]$中完全分解成线性因式的乘积。

证 设$f(X)$在$F[X]$中不能分解成线性因式的乘积。令α是$f(X)$在F的某一个代数闭包Ω内的一个根。且$\alpha\notin F$。那么由3.7.4，$K=F(\alpha)$是一个p次循环扩域。这样一来，$f(X)$就是α在F上的最小多项式；因而$f(X)$不可约。 ▮

现在我们来讨论情形2。这时要对基础域F作一点限制，即要求 **F 含有一个本原n次单位根。**

注意由3.4.1，(iv)，如果F含有一个本原n次单位根，必须有char$F=0$或char$F=p$，而$p\nmid n$。因此只能是情形2。

我们先证明一个引理。

引理 3.7.6 设 n 是一个正整数，域 F 含有一个本原 n 次单位根 ζ. 如果 d 是 n 的一个正因子而 $\alpha\neq 0$ 是 F 上多项式 X^d-a 的一个根. 那么 X^d-a 有 d 个两两不同的根，$\alpha, \eta\alpha, \cdots, \eta^{d-1}\alpha$，这里 η 是一个本原 d 次单位根，而 $K=F(\alpha)$ 是多项式 X^d-a 在 F 上的分裂域，并且是 F 的一个 Galois 扩域.

证 因为 F 含有一个本原 n 次单位根 ζ，而 $d|n$，所以 $\eta==\zeta^{n/d}\in F$ 是一个本原 d 次单位根. 设 $\alpha\neq 0$ 是 $X^d-a\in F[X]$ 的一个根. 那么 $\alpha, \eta\alpha, \cdots, \eta^{d-1}\alpha$ 是 X^d-a 在 $F(\alpha)$ 里的一切根，且两两不同. 因此，$F(\alpha)$ 是可分多项式 X^d-a 在 F 上的分裂域，因而是 F 的一个 Galois 扩域. ▮

定理 3.7.7 设 n 是一个正整数. 域 F 含有一个本原 n 次单位根 ζ. 对于 F 的一个扩域 K 来说，以下三个条件是等价的:

（i） K 是 F 上一个形如 X^d-b 的不可约多项式在 F 上的分裂域，其中 $d|n$. 这时 $K=F(\beta)$，β 是 X^d-b 的任意一个根.

（ii） K 是 F 上一个形如 X^n-a 的多项式在 F 上的分裂域. 这时 $K=F(\alpha)$，α 是 X^n-a 的任意一个根.

（iii） K 是 F 的一个 d 次循环扩域，其中 $d|n$.

证 (i)$\Longrightarrow$(ii) 设 α 是 F 上不可约多项式 X^d-b 在 K 中的一个根，$d|n$. 由3.7.6，$K=F(\alpha)$ 是 X^d-b 在 F 上的分裂域. 又 $(\zeta\alpha)^n=\alpha^n=b^{n/d}\in F$. 令 $a=b^{n/d}$. 则 $\zeta\alpha$ 是 $X^n-a\in F[X]$ 在 K 中的根. 再由3.7.6，$F(\zeta\alpha)$ 是 X^n-a 在 F 上的分裂域. 然而 $\zeta\in F$，所以 $F(\zeta\alpha)=F(\alpha)=K$，并且 $\zeta^i\alpha(0\leqslant i\leqslant n-1)$ 就是 X^n-a 的全部根，它们都属于 K. $K=F(\zeta^i\alpha)$，$i=0,1,\cdots,n-1$.

(ii)$\Longrightarrow$(iii) K 是多项式 $X^n-a\in F[X]$ 在 F 上的分裂域. 令 $\alpha\in K$ 是 X^n-a 的任意一个根. 由3.7.6，$K=F(\alpha)$ 是 Galois 扩域，而 $\alpha, \zeta\alpha, \cdots, \zeta^{n-1}\alpha$ 是 X^n-a 的全部根. 设 $\sigma\in(K/F)$. 那么 $\sigma(\alpha)=\zeta^i\alpha$，对某一个 i，$0\leqslant i\leqslant n-1$.

$$\theta: G\ni\sigma\longmapsto\zeta^i\in W_n，若\sigma(\zeta)=\zeta^i,$$

这里 $W_n=\{1,\zeta,\cdots,\zeta^{n-1}\}$ 是 n 次单位根群。则 θ 是一个群同态单射。因而 G 与 n 阶循环群 W_n 的一个子群同构，所以 G 是一个 d 阶循环群，这里 d 是 n 的一个因子。

(iii)$\Longrightarrow$(i) $G=G(K/F)$ 是一个 d 阶循环群，$d|n$。令 σ 是 G 的一个生成元。$\eta=\zeta^{n/d}\in F$ 是一个本原 d 次单位根。因为 $N_F^K(\eta)=\eta^{[K:F]}=\eta^d=1$，由 3.7.2，存在 $\beta\in K$，使得 $\eta=\beta\sigma(\beta)^{-1}$。令 $\alpha=\beta^{-1}$。则 $\sigma(\alpha)=\eta\alpha$，$\sigma(\alpha^d)=(\eta\alpha)^d=\alpha^d$。所以 $\alpha^d=b\in F$。因此 α 是 F 上多项式 X^d-b 的一个根。由 3.7.6，$F(\alpha)\subseteq K$ 是 X^d-b 在 F 上的分裂域，$\alpha,\eta\alpha,\cdots,\eta^{d-1}\alpha$ 是 X^d-b 的全部根，并且都属于 K。对于每一个 i，$0\leqslant i\leqslant d-1$，$\sigma^i(\alpha)=\eta^i\alpha$，所以 $\sigma^i: F(\alpha)\to F(\eta^i\alpha)$ 是 F-同构。由 2.2.7，α 与 $\eta^i\alpha$ 是 F 上同一个不可约多项式的根，$0\leqslant i\leqslant d-1$。这样，$X^d-b$ 是 F 上不可约多项式。所以 $[F(\alpha):F]=d=[K:F]$，$K=F(\alpha)$。

注意 在上面定理3.7.7的证明里，基础域 F 含有一个本原 n 次单位根这一条件起着重要的作用。当 F 上不含本原 n 次单位根时，对多项式 $X^n-a\in F[X]$ 在 F 上的分裂域的刻画要困难得多。当 $a=1$ 时，就是前一节所讨论的分圆扩域。

习 题

1. 设 F 是一个域，char$F\neq 2$。又设 $a\in F$ 而 $b=1+a^2\notin F^2$。证明，$K=F(\sqrt{b+\sqrt{b}})$ 是 F 的四次循环扩域，它的Galois群由 K 的 F-自同构

$$\sigma: \sqrt{b+\sqrt{b}}\longmapsto\sqrt{b-\sqrt{b}}$$

生成。

2. 设 F 是一个域。又设存在 $b,c\in F$ 使得 $a=b^2+c^2\notin F^2$，证明，$K=F(\sqrt{a+b\sqrt{a}})$ 是 F 的四次循环扩域。求出它的Galois群的一个生成元。

3. 令 $\overline{Q}$ 是域 Q 的一个固定的代数闭包，$\alpha\in\overline{Q}$ 但 $\alpha\notin\overline{Q}$。设

E 是 $\overline{\mathbf{Q}}$ 中不含 α 的最大子域。证明，E 的每一个有限次扩域都是循环扩域。

4. 设 F 是一个域，Ω 是 F 的一个代数闭包，$\sigma \in G(\Omega/F)$。令

$$K=\{\alpha \in \Omega \mid \sigma(\alpha)=\alpha\}.$$

证明，K 是一个域，并且 K 的每一个有限次扩域都是循环扩域。

5. 设 p 是一个素数，K 是域 F 的一个 p^n 次循环扩域，$E \subset K$ 并且是 F 的 p^{n-1} 次循环扩域。又设 $\alpha \in K$ 使得 $K=E(\alpha)$。证明，$K=F(\alpha)$。

6. 设 p 是一个素数，F 是一个域。

(i) 如果 $\mathrm{char}F=p$，或者 $\mathrm{char}F\neq p$，但 F 含有一个本原 p 次单位根，那么 $X^p-a\in F[X]$ 或者不可约，或者在 $F[X]$ 内可以分解成一次因式的积。

(ii) 设 $\mathrm{char}F=p$，而 α 是 $X^p-a\in F[X]$ 的任意一个根。证明

$$F(\alpha)\neq F(\alpha^p)\Longleftrightarrow[F(\alpha):F]=p.$$

7. 设 F 是一个域且 $\mathrm{char}F=p>0$。令 $F_p=\{a^p-a \mid a\in F\}$。证明：

(i) 存在 F 的一个 p 次循环扩域的充要条件是 $F\neq F_p$；

(ii) 如果存在 F 的一个 p 次循环扩域，那么对于任意 $n\geq 1$，都存在 F 的 p^n 次循环扩域。

8. 设 p 是一个素数，K 是域 F 上一个 p 次可分扩域。证明，存在 F 的一个有限次扩域 M，使得 KM 是 M 的一个 p 次循环扩域。

3.8 关于有限群的若干结果

我们以下将要讨论一个系数在某个域内的代数方程在什么时候可以用“根号解”的问题。在此之前，需要关于有限群的一些

预备知识。

首先证明关于交错群的一个性质。

一个群 G 叫做**单群**，如果除开 G 本身和单位子群 $\{1\}$ 外，G 没有其它的正规子群。因为一个 Abel 群的子群都是正规的。所以一个 Abel 群是单的必要且只要它没有异于它本身和 $\{1\}$ 的真子群。

显然，素数阶的循环群是单的 Abel 群。反过来，任何一个有限的单 Abel 群 $G\neq\{1\}$ 一定是某一素数阶的循环群。事实上，设 $a\in G$，$a\neq 1$，则 a 生成 G 的一个循环子群 $\langle a\rangle$。$\langle a\rangle\neq\{1\}$ 所以必须 $\langle a\rangle=G$。如果 a 的阶 $n=|G|$ 是一个合数。则 $n=n_1n_2$，$1<n_1<n$，$1<n_2<n$。于是 a^{n_1} 生成 G 的一个 n_2 阶的真子群，这与 G 的单性矛盾。

最简单的一类非 Abel 单群就是 $n\geqslant 5$ 时，交错群 A_n。为了证明 $A_n(n\geqslant 5)$ 是单群，先证明两个引理。

引理 3.8.1 设 $n\geqslant 3$。令 i，j 是 $\{1,2,\cdots,n\}$ 中不同的元素。则 A_n 由一切3-轮换 $\{(i,j,k)\mid 1\leqslant k\leqslant n;\ k\neq i,j\}$ 生成。

证 $n=3$ 时是显然的。设 $n>3$。因为 A_n 是由一切 n 次偶置换组成，所以 A_n 的每一个元素都可以表示成形如

$$(ab)(cd)\text{或}(ab)(ac)$$

的乘积，这里 a,b,c,d 是 $\{1,2,\cdots,n\}$ 中互不相同的元素。然而

$$(ab)(cd)=(acb)(acd),$$
$$(ab)(ac)=(acb).$$

所以 A_n 由一切3-轮换生成。每一个3-轮换都具有下列形式之一：

$$(ija),(iaj),(iab),(jab),\text{或}(abc),$$

这里 $a,b,c\neq i$ 或 j，且互不相同。因为

$$(iaj)=(ija)^2,(iab)=(ijb)(ija)^2,$$
$$(jab)=(ijb)^2(ija),\quad (abc)=(ija)^2(ijc)(ijb)^2(ija),$$

所以 A_n 由 $\{(ijk)\mid 1\leqslant k\leqslant n,k\neq i,j\}$ 生成。 ∎

引理 3.8.2 设$n\geqslant 3$而N是A_n的一个正规子群．如果N含有一个3-轮换，则$N=A_n$．

证 设N含有一个3-轮换(ijk)．那么对于任意l，$1\leqslant l\leqslant n$，$l\neq i,j,k$，我们有

$$(ijl)=(ij)(kl)(ijk)^2(kl)(ij)\in N.$$

因而N含有一切(ijk)，$1\leqslant k\leqslant n$，$k\neq i,j$，由3.8.1，$N=A_n$．

定理 3.8.3 当$n\geqslant 5$时，A_n是单群．

证 设N是A_n的一个正规子群．且$N\neq\{1\}$，我们证明，N一定含有一个3-轮换，从而由3.8.2，$N=A_n$．我们分别就以下情况来考虑：

1. 如果N含有一个3-轮换，这时已无须证明．

2. $N\ni\sigma$，而σ被表成不相交的轮换的积时，至少有一个长度$r\geqslant 4$的轮换．这时

$$\sigma=(a_1a_2\cdots a_r)\tau.$$

令$\delta=(a_1a_2a_3)\in A_n$．则

$$N\ni\sigma^{-1}\delta\sigma\delta^{-1}=(a_1a_3a_r).$$

3. $N\ni\sigma$，而σ被表成不相交的轮换的积时，至少有两个因子是3-轮换．这时

$$\sigma=(a_1a_2a_3)(a_4a_5a_6)\tau.$$

令$\delta=(a_1a_2a_4)\in A_n$．则

$$N\ni\sigma^{-1}\delta\sigma\delta^{-1}=(a_1a_4a_2a_6a_3).$$

于是由情形2，N含有一个3-轮换．

4. $N\ni\sigma$，σ是一个3-轮换和一些2-轮换(不相交)的积．这时$\sigma=(a_1a_2a_3)\tau$，τ是一些2-轮换的积，于是

$$N\ni\sigma^2=(a_1a_2a_3)^2\tau^2=(a_1a_2a_3)^2=(a_1a_3a_2).$$

5. 设N的每一个元素都是一些不相交的2-轮换的积．设$\sigma\in N$．则

$$\sigma=(a_1a_2)(a_3a_4)\tau,$$

这里 τ 是一些不相交的2-轮换的积，且不出现a_1,a_2,a_3,a_4。令 $\delta=(a_1a_2a_3)\in A_n$。则

$$N\ni\sigma^{-1}\delta\sigma\delta^{-1}=(a_1a_3)(a_2a_4).$$

因为 $n\geqslant5$，所以存在 $b\in\{1,2,\cdots,n\}$且 $b\neq a_1,a_2,a_3,a_4$，令$\alpha=$ $=(a_1a_3b)\in A_n$，$\beta=(a_1a_3)(a_2a_4)\in N$。则

$$N\ni\beta^{-1}\alpha\beta\alpha^{-1}=(a_1a_3b).$$

以上五种情形穷尽了N中元素一切可能的形式，这样，A_n没有非平凡正规子群，因而是单群。 ∎

现在介绍可解群的概念。

设G是一个群。一个子群序列

$$(1)\qquad G=G_0\supseteq G_1\supseteq\cdots\supseteq G_s=\{1\},$$

其中每一个 G_i 都是 G_{i-1} 的正规子群，$1\leqslant i\leqslant s$，叫做 G 的一个**正规列**。

例如，$S_3\supset A_3\supset\{1\}$是三次对称群$S_3$的一个正规列。而

$$S_4\supset A_4\supset V\supset W\supset\{1\},$$

这里$V=\{1,(12)(34),(13)(24),(14)(23)\}$，$W=\{1,(12)(34)\}$，是四次对称群 S_4 的一个正规列。

给了G的一个正规列(1)，相应地就得到一个商群序列

$$(2)\qquad G/G_1,G_1/G_2,\cdots,G_{s-1}/G_s\cong G_{s-1}.$$

一个群G叫做一个**可解群**，如果G有一个正规列(1)，而且每一个商群G_{i-1}/G_i都是Abel群，($1\leqslant i\leqslant s$)。

例如，在上面所给出的S_3和S_4的正规列里，S_3/A_3是2阶循环群，A_3是3阶循环群，S_4/A_4是2阶循环群，A_4/V是3阶循环群。V/W和W都是2阶循环群，它们都是Abel群。因此S_3和S_4**都是可解群**。另外，Abel群自然都是可解群。

我们还要给出可解群的另一个等价的定义。首先引入导出列的概念。

令G是一个群。令$G^{(1)}=[G,G]$是G的换位子群，即是由G

的一切换位子$aba^{-1}b^{-1}(a,b\in G)$所生成的子群。$G^{(1)}$是G的一个正规子群，因为对于$a\in G$和$b\in G^{(1)}$，我们有$aba^{-1}=aba^{-1}b^{-1}b\in G^{(1)}$。

设$n>1$。如果$G^{(n-1)}$已被定义，我们定义$G^{(n)}=[G^{(n-1)},G^{(n-1)}]$。这样，我们就得到$G$的一个子群序列

(3) $$G=G^{(0)}\supseteq G^{(1)}\supseteq G^{(2)}\supseteq\cdots\supseteq G^{(n)}\supseteq\cdots.$$

序列(3)叫做G的**导出列**。

根据换位子群的定义可知，(3)中每一个商群$G^{(i-1)}/G^{(i)}$都是Abel群，$i\geqslant 1$。

定理 3.8.4 一个群G是可解的必要且只要存在一个正整数n，使得$G^{(n)}=\{1\}$。

证 如果G是可解群，那么G有一个正规列(1)，其中每一个商群G_{i-1}/G_i都是Abel群$(1\leqslant i\leqslant s)$。因为$G/G_1$是Abel群，所以对于任意$a,b\in G$，我们有$aba^{-1}b^{-1}\in G_1$，所以$G^{(1)}\subseteq G_1$。一般，由$G_{i-1}/G_i$是Abel群可以推出$G^{(i)}\subseteq G_i$。取$n=s$，则$G^{(n)}=\{1\}$。

反之，设有某一个$n>0$使得$G^{(n)}=\{1\}$。则

$$G=G^{(0)}\supseteq G^{(1)}\supseteq\cdots\supseteq G^{(n)}=\{1\}$$

是G的一个正规列，且$G^{(i-1)}/G^{(i)}$是Abel群，$1\leqslant i\leqslant n$，所以G是可解群。 ▮

推论 3.8.5 可解群的任意子群和任意同态像都是可解群。

证 设对某一个$n>0$，$G^{(n)}=\{1\}$。令H是G的一个子群。则$H^{(i)}\subseteq G^{(i)}$，从而$H^{(n)}=\{1\}$。

设N是G的一个正规子群，则对任意$i>0$，

$$(G/N)^{(i)}=NG^{(i)}/N.$$

于是$(G/N)^{(n)}=N/N=\{1\}$。 ▮

定理 3.8.6 设N是群G的一个正规子群。G是可解群必要且只要N和G/N都是可解群。

证 由3.8.5，若G是可解群，则N和G/N都是可解群。反之，由于G/N可解，所以G/N有正规列

$$G/N=G_0/N\supseteq G_1/N\supseteq\cdots\supseteq G_s/N=\{1\},$$

商群$G_{i-1}/G_i\cong(G_{i-1}/N)/(G_i/N)$是Abel群，$1\leqslant i\leqslant s$。又因为$N$可解，所以$N$有正规列

$$N=N_0\supseteq N_1\supseteq\cdots\subseteq N_t=\{1\}.$$

商群N_{j-1}/N_j是Abel群，$1\leqslant j\leqslant t$。于是

$$G\supseteq G_1\supseteq\cdots\supseteq G_s=N\supseteq N_1\supseteq\cdots\supseteq N_t=\{1\}$$

是满足可解群定义的一个正规列。 ▮

推论 3.8.7 设$H_1,\cdots,H_s$是群G的正规子群。令$N=\bigcap_{i=1}^{s}H_i$。如果每一个商群$G/H_i(1\leqslant i\leqslant s)$都是可解群，则$G/N$也是可解群。

证 对s作归纳法。对于任意$i\neq j$，$1\leqslant i,j\leqslant s$，我们有

$$G/H_j\supseteq H_iH_j/H_j\cong H_i/H_i\cap H_j.$$

所以$H_i/H_i\cap H_j$与可解群G/H_j的一个子群同构，因而是可解群，另一方面，

$$(G/H_i\cap H_j)/(H_i/H_i\cap H_j)\cong G/H_i$$

也是可解群。于是由3.8.6，$G/H_i\cap H_j$是可解群。

假设$s>2$，并且已知$G/\bigcap_{i=1}^{s-1}H_i$是可解群。令$M=\bigcap_{i=1}^{s-1}H_i$。于是

$$G/M\supseteq MH_s/M\cong H_s/M\cap H_s=H_s/N.$$

因此H_s是可解群。又因为

$$(G/N)/(H_s/N)\cong G/H_s$$

可解，所以由3.8.6，G/N是可解群。 ▮

定理 3.8.8 设$G\neq\{1\}$是一个有限群。G是可解的必要且只要存在一个正规列

$$G=G_0\supseteq G_1\supseteq\cdots\supseteq G_s=\{1\},$$

其中每一个商群$G_{i-1}/G_i(1\leqslant i\leqslant s)$都是素数阶的循环群。

证 设G是可解群。于是G有一个正规列

$$G=G_0\supseteq G_1\supseteq\cdots\supseteq G_s=\{1\},$$

其中每一个$G_{i-1}/G_i(1\leqslant i\leqslant s)$都是Abel群。在商群$G/G_1$中存在一个异于$G/G_1$的最大阶的正规子群$N_1/G_1$。如果$N_1\neq G$，那么在商群$N_1/G_1$中存在一个异于$N_1/G_1$的最大阶的正规子群$N_2/G_1$。如此继续下去，最后一定有某一个$t>0$，使得$N_t=G_1$。这样就得到一个子群序列

$$G=N_0\supsetneqq N_1\supsetneqq\cdots\supsetneqq N_t=G_1.$$

N_{i-1}/N_i是单Abel群，所以是一个素数阶循环群，$1\leqslant i\leqslant t$。再对G_1/G_2，G_2/G_3，… 作同样的考虑。最后我们得到G的一个正规列

$$G=N_0\supseteq N_1\supseteq\cdots\supseteq N_m=\{1\},$$

其中每一个商群N_{i-1}/N_i都是素数阶的循环群。

反过来是显然的。 ▌

最后，由3.8.3，我们立即得到

定理 3.8.9 当$n\geqslant 5$时，n次对称群S_n不是可解群。

证 如果S_n可解，则A_n可解。然而由3.8.3，当$n\geqslant 5$时，A_n没有非平凡的正规子群，且A_n不是Abel群，所以A_n不可能有满足可解群定义的正规列。 ▌

3.9 可解扩域和根号扩域

设F是一个域。F的一个Galois扩域K叫做F的一个**可解扩域**，如果K/F的Galois群$G(K/F)$是一个可解群，这时K/F叫做一个**可解扩张**。

例 1 Abel扩张都是可解扩张。

例 2 $K=Q(\sqrt[3]{2},\sqrt{-3})$是$Q$的一个可解扩域。因为$K/Q$是Galois扩张，它的Galois群$G(K/Q)$与$S_3$同构，后者是一个

可解群（3.2例4）。

定理 3.9.1 设M是域F的一个扩域。K和L都是M/F的中间域。如果K和L都是F的有限次可解扩域，那么合成域KL也是F的一个有限次可解扩域。

证 因为K/F和L/F都是有限次Galois扩张，所以由3.1.9，KL/F也是有限次Galois扩张。令$G=G(KL/F)$，$N=G(KL/L)$。由3.3.4，N是G的正规子群，且$G/N\cong G(L/F)$。由题设，G/N是可解群。又由3.1.9，

$$N=G(KL/L)\cong G(K/K\cap L)\subseteq G(K/F).$$

所以N也是可解群。于是由3.8.6，G是可解群，从而KL是F可解扩域。 ▮

定理 3.9.2 设F是一个域，Ω是F的一个代数闭包。令$F\subseteq K\subseteq L\subseteq\Omega$是一串扩域，其中$K$是$F$的有限次可解扩域而$L$是$K$的有限次可解扩域。那么存在$F$的一个有限次可解扩域$M$，使得$F\subseteq K\subseteq L\subseteq M\subseteq\Omega$。

证 L/K和K/F都是有限次可分扩张，所以L/F也是有限次可分扩张。于是由3.1.5，存在F的一个有限次Galois扩域P，使得

$$F\subseteq K\subseteq L\subseteq P\subseteq\Omega.$$

令$G=G(P/F),N=G(P/K),H=G(P/L)$，则$H\lhd N$，$N\lhd G$，我们有

$$N/H\cong G(L/K),\quad G/N\cong G(K/F).$$

所以N/H，G/N都是可解群。设$H_1,\cdots,H_s$是G中一切与H共轭的子群，令$U=\bigcap_{i=1}^{s}H_i$。因为$N\lhd G,H\lhd N$,所以$H_i\lhd N$，且$N/H_i\cong N/H$，因此N/H_i是可解群，$1\leqslant i\leqslant s$。于是由3.8.7，N/U是可解群。

令M是与G的子群U相对应的P/F的中间域。则

$[M:F]\leqslant[P:F]<\infty$。$U\cong G(P/M)$。$U\subseteq H$，所以 $M\supseteq L$。又因为$U\lhd G$，所以M是F的Galois扩域，且$G(M/F)\cong G/U$。这些子群与中间域的对应关系如下：

$$P\longleftrightarrow\{1\}$$
$$M\longleftrightarrow U$$
$$L\longleftrightarrow H$$
$$K\longleftrightarrow N$$
$$F\longleftrightarrow G$$

我们有

$$(G/U)/(N/U)\cong G/N\cong G(K/F).$$

而 N/U，G/N 都可解，所以由 3.8.6，G/U 是可解群。于是 $G(M/F)$是可解群。这样一来，M就是F的一个满足定理要求的有限次可解扩域。 ▮

现在我们引入根号扩域的概念。

设F是一个域。F的一个扩域K叫做F的一个**根号扩域**，(K/F称为根号扩张)如果存在K/F的一串中间域 $F=F_0$，F_1，⋯ $F_r=K$：

$$F=F_0\subseteq F_1\subseteq\cdots\subseteq F_r=K,$$

使得$F_i=F_{i-1}(\alpha_i)$，$\alpha_i^{n_i}\in F_{i-1}$，其中$n_i$是一个不能被 char$F$ 整除的正整数，$1\leqslant i\leqslant r$。

由定义立即得出以下简单事实：

1. 域F的根号扩域一定是有限次扩域。
2. 如果K/F和L/K都是根号扩张，则L/F也是根号扩张。
3. 设K是F的一个根号扩域，而K'是K在F上一个与K共轭的域，则K'也是F的根号扩域。
4. 设K和L都被包含在F的一个共同的扩域内。如果K/F，L/F都是根号扩张，则KL/F也是根号扩张。

可解扩张和根号扩张之间的关系由以下定理指出。

定理 3.9.3 设F是一个域，Ω是F的一个代数闭包。

（i） 设$K(\subseteq\Omega)$是F的一个根号扩域。那么存在F的一个有限次可解扩域L，使得$F\subseteq K\subseteq L\subseteq\Omega$。

（ii） 设$K(\subseteq\Omega)$是F的一个有限次可解扩域，且$[K:F]$不能被 char$F$ 整除。那么存在 F 的一个根号扩域 L，使得$F\subseteq K\subseteq L\subseteq\Omega$。

证 （i） 对域次数$n=[K:F]$作归纳法来证明L的存在。

$n=1$时，$K=F$，这时取$L=K=F$即可。

设$n>1$。假定存在K/F的中间域序列：

$$F=F_0\subseteq F_1\subseteq\cdots\subseteq F_r=K,$$

$F_i=F_{i-1}(\alpha_i),\alpha_i^{n_i}\in F_{i-1}$，char$F\nmid n_i$， 且 $[F_i:F_{i-1}]>1$ $(1\leqslant i\leqslant r)$。令$K'=F_{r-1}$。则$K'\neq K,K=K'(\alpha)$。$\alpha^m\in K'(\alpha=\alpha_r,m=n_r)$。则$[K':F]<[K:F]$且$K'/F$是根号扩张。由归纳法的假设，存在$F$的有限次可解扩域$L'$，使得

$$F\subseteq K'\subseteq L'\subseteq\Omega.$$

因为char $F\nmid m$，所以Ω含有一个本原m次单位根ζ。令$P=F(\zeta)\subseteq\Omega$。由3.5.2，$P$是$F$的有限次 Abel 扩域，又$L'$是$F$的有限次可解扩域。于是由3.9.1，$M=L'P=L'(\zeta)$是$F$的一个有限次可解扩域。

因为$\alpha^m\in K'\subseteq L'\subseteq M$，且$\zeta\in P\in M$。所以由3.7.7，$M(\alpha)$是$M$的一个有限次循环扩域，因而是$M$的一个有限次可解扩域。在扩域序列$F\subseteq M\subseteq M(\alpha)\subseteq\Omega$里，$M/F$，$M(\alpha)/M$都是有限次可解扩张，由3.9.2，存在$F$的一个有限次可解扩域$L$，使得

$$F\subseteq M\subseteq M(\alpha)\subseteq L\subseteq\Omega.$$

因为$K=K'(\alpha)\subseteq L'(\alpha)\subseteq M(\alpha)$，所以$F\subseteq K\subseteq L\subseteq\Omega$。

（ii） 仍是对$n=[K:F]$，char$F\nmid n$，作数学归纳法来证明L的存在。

$n=1$时显然。这时$K=F$。$L=K=F$。

设 $n>1$，且 $\mathrm{char}F\nmid n$。令 $G=G(K/F)$。则 G 是有限可解群。于是由3.8.8，存在 G 的一个正规列

$$G=N_0\supseteq N_1\supseteq\cdots\supseteq N_r=\{1\}.$$

其中每一个商群 N_{i-1}/N_i 都是阶为某一素数 q_i 的循环群，$1\leqslant i\leqslant r$。因为 $\mathrm{char}F\nmid n$，而 $q_i|n$，所以 $\mathrm{char}F\nmid q_i(1\leqslant i\leqslant r)$。

记 $N=N_1$，$N\lhd G$，商群 G/N 是素数 $q=q_1$ 阶的循环群。令 K' 是 K/F 中与 N 对应的中间域。则 $G(K/K')=N, G(K'/F)\cong G/N$，所以 K' 是 F 的 q 次循环扩域。

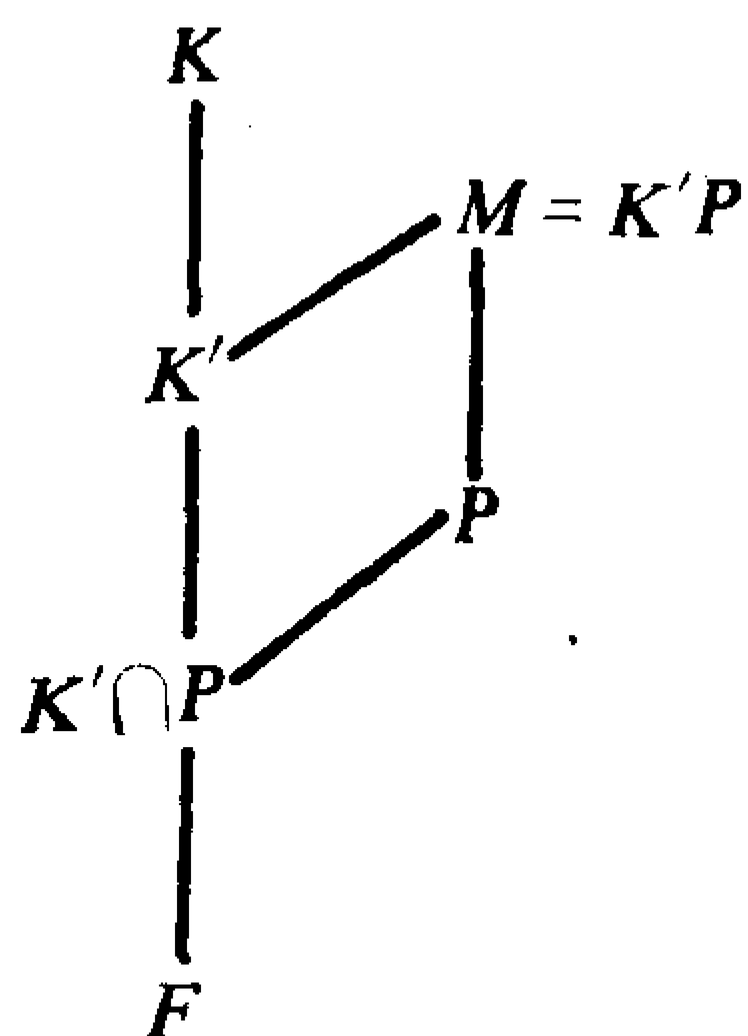
因为 $\mathrm{char}F\nmid q$，所以 Ω 含有一个本原 q 次单位根 η。令 $P=F(\eta)$，$M=K'P=K'(\eta)$。因为 K'/F 是有限次 Galois 扩张，所以由3.1.9，$M=K'P$ 是 P 的 Galois 扩域，且

$$G(M/P)\cong G(K'/K'\cap P)\subseteq G(K'/F)\cong G/N.$$

因为 G/N 是素数 q 阶的循环群，所以 $|G(M/P)|=q$ 或 1.

如果 $|G(M/P)|=q$，则 $G(M/P)$ 是 q 阶循环群。于是 M 是 P 的 q 次循环扩域，而 $\eta\in P$，所以由3.7.6和3.7.7，存在 $\alpha\in M$，使得 $\alpha^q\in P$。

如果 $|G(M/P)|=1$，则 $M=P$。



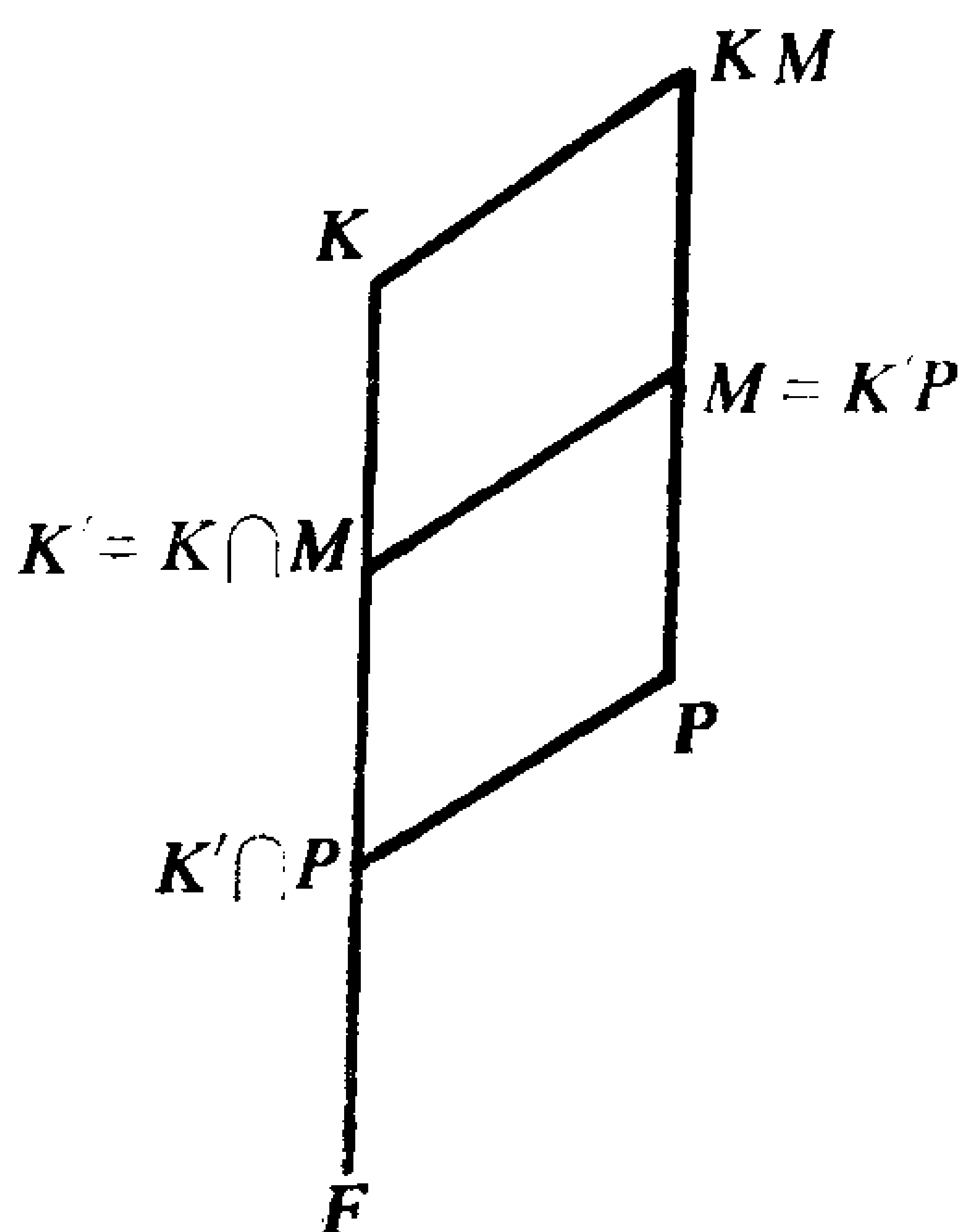
不论哪一个情形，M 都是 P 的根号扩域。又 $P=F(\eta)$ 是 F 的根号扩域。所以 M 是 F 的根号扩域。

因为 K/F 是有限次 Galois 扩张，所以由3.1.9，KM/M 也是 Galois 扩张，并且

$$G(KM/M)\cong G(K/K\cap M)$$

$$\subseteq G(K/F).$$

由于 $G(K/F)$ 是有限可解群，所以 $G(KM/M)$ 也是有限可解群，从而 KM 是 M 的有限次可解扩域，因为 $M=K'P$，所以 $K'\subseteq K\cap M$。



因此
$[KM:M]=[K:K\cap M]$ 可以整除 $[K:K']=[K:F]/[K':F]=n/q<n$。因为 $\mathrm{char}F\nmid n$，所以 $\mathrm{char}F\nmid[KM:M]$。

于是，由归纳法的假设，存在 M 的一个根号扩域 L，使得 $M\subseteq KM\subseteq L\subseteq\Omega$。然而 M 是 F 的根号扩域，所以 L 是 F 的根号扩域。定理被证明。▌

习　题

1. 设 F 是一个特征为零的域，$f(X)\in F[X]$ 是一个 n 次不可约多项式，$n\geqslant5$，K 是 $f(X)$ 在 F 上的分裂域，且 $G(K/F)\cong S_n$。令 α 是 $f(X)$ 在 K 内的一个根。

(i) $F(\alpha)/F$ 是不是 Galois 扩张？

(ii) $G(F(\alpha)/F)$ 是不是可解群？

(iii) 是否存在 F 上根号扩域 E，使得 $E\supset F(\alpha)\supset F$？

2. 设 K 是域 F 的一个根号扩域，L 是 K/F 的 Galois 闭包。证明，L 也是 F 的根号扩域。

3. 设 p 是一个素数，F 是一个域但 $\mathrm{char}F\neq p$。证明，$X^p-a\in F[X]$ 或者在 F 上不可约，或者在 F 内有一个根。

3.10 代数方程的根号解

Galois 理论起源于一个古典的方程论问题：给了某一个数域 F 上的代数方程 $f(X)=0$，$f(X)\in F[X]$，是否存在一个由

对于 $f(X)$ 的系数施行有限次加、减、乘、除及开方运算所组成的公式，使得这个方程的每一个根都可以由这个公式表示出来？

假设这样一个公式存在。由于加、减、乘、除运算可以在基础域里进行，而对一个数 a 开 n 次方相当于求一个数 α，使得 $\alpha^n=a$，因此，存在一串扩域

$$F=F_0\subseteq F_1\subseteq\cdots\subseteq F_r=K,$$

其中 $F_i=F_{i-1}(\alpha_i)$，$\alpha_i^{n_i}\in F_i(1\leqslant i\leqslant r)$，使得 $f(X)$的每一个根都在K内。这相当于说，存在F的一个根号扩域K，使得$f(X)$的每一个根都包含在K内。

反过来，设 $f(X)$是数域F上一个多项式。如果存在F的一个根号扩域K，使得 $f(X)$的每一个根都包含在K内，那么一定存在方程 $f(X)=0$ 的根的表达式，这个表达式是由 $f(X)$ 的系数经过有限次加、减、乘、除及开方运算组成的。

一般，设 F 是任意一个域。$f(X)\in F[X]$。方程 $f(X)=0$ **说是在 F 上可以用根号解**，如果存在F的一个根号扩域K，使得 $f(X)$的全部根都在K内。

由前一节的结果。很容易得出域F上一个方程在F上可以用根号解的充要条件。首先注意一个简单的事实。

引理 3.10.1 设F是一个域，$f(X)$是$F[X]$中一个次数大于零的多项式，L是$f(X)$在F上一个分裂域。如果 char$F$ 不能整除$[L:F]$，则L是F的一个calois 扩域。

证 只要证明L/F是可分扩张。当 char$F=0$ 时显然。设 char$F=p>0$。令α是L的任意元素。则$[F(\alpha):F]\mid[L:F]$。因为 $p\nmid[L:F]$，所以$p\nmid[F(\alpha):F]$。所以$F(\alpha)$是F的可分扩域，因而α是F上可分元素。所以L是F上可分扩域。 ∎

定理 3.10.2 设F是一个域，$f(X)\in F[X]$是一个次数大于零的多项式，L是$f(X)$在F上一个分裂域，且char$F\nmid[L:F]$。那么方程 $f(X)=0$ 在F上可以用根号解必要且只要L是F的一

个有限次可解扩域.

证 设$f(X)=0$在F上可以用根号解. 于是存在F的一个根号扩域K, 使得$F\subseteq L\subseteq K$. 由3.9.3, 存在F的一个有限次可解扩域M, 使得$F\subseteq K\subseteq M$. 从而有$F\subseteq L\subseteq M$.

因为M/F是有限次可解扩张, 又由3.10.1, L/F是Galois扩张, 所以$G(M/F)$是可解群, 且$G(M/L)\lhd G(M/F)$. 于是

$$G(L/F)\cong G(M/F)/G(M/L)$$

是可解群, 因而L是F的有限次可解扩域.

反之, 设$L=F(\alpha_1,\cdots,\alpha_m)$是多项式$f(X)$在$F$上的分裂域. 由题设, L/F是有限次可解扩张, 且$\operatorname{char}F\nmid[L:F]$. 由3.9.3, 存在$F$的一个根号扩域$K$, 使得$F\subseteq L\subseteq K$. 所以$f(X)=0$的全部根都包含在$F$的一个根号扩域内, 因而$f(X)=0$可以用根号解. ∎

设F是一个域, $f(X)\in F[X]$是F上一个可分多项式. 令L是$f(X)$在F上一个分裂域. L自然是F的Galois扩域. Galois群$G(L/F)$叫做**多项式$f(X)$的**(或**方程$f(X)=0$的**)**Galois群**.

这个定义不依赖于分裂域L的选取. 事实上, 设L和L'都是$f(X)$在F上分裂域. 那么L与L'是F-同构的. 所以$G(L/F)\cong G(L'/F)$. 因此, 多项式$f(X)\in F[X]$的Galois群除同构外是唯一确定的.

如同定理3.10.2的证明一样, 我们得到以下

定理 3.10.3 设$f(X)$是域F上一个可分多项式.

(i) 如果方程$f(X)=0$在F上可以用根号解, 则方程$f(X)=0$的Galois群G是一个可解群.

(ii) 如果方程$f(X)=0$的Galois群G是可解群, 并且$\operatorname{char}F$不能整除G的阶, 则方程$f(X)=0$在F上可以用根号解. ∎

推论 3.10.4 设F是一个特征为0的域。$f(X)$是F上一个多项式，方程$f(X)=0$在F上可以用根号解必要且只要方程$f(X)=0$的Galois群是可解群。 ▮

习 题

1. 设F是一个域，$\mathrm{char}F\neq 2$，$f(X)\in F[X]$是一个最高次项系数为1的$n(>0)$次可分多项式，$\alpha_1,\cdots,\alpha_n$是$f(X)$在F的某一个扩域内的全部根，$K=F(\alpha_1,\cdots,\alpha_n)$。令

$$d=\prod_{1\leqslant i<j\leqslant n}(\alpha_i-\alpha_j).$$

G是$f(X)$的Galois群。将G看作S_n的一个子群。证明，在Galois基本定理中与子群$G\cap A_n$对应的中间域是$F(d)$。

2. 在前题的假设和记号下，令

$$D=\prod_{1\leqslant i<j\leqslant n}(\alpha_i-\alpha_j)^2.$$

证明，$G\subset A_n$必要且只要D是F中某个元素的平方（D称为$f(X)$的判别式）。

3.11 n次一般方程

我们将证明，当$n>4$时，特征为0的域上n次一般方程不能用根号解。

先证明一个引理。

引理 3.11.1 设k是一个域，$K=k(x_1,\cdots,x_n)$是k上n个不相关不定元$x_1,\cdots,x_n$的有理分式域。令

$$a_1=\sum_{i=1}^{n}x_i,\quad a_2=\sum_{1\leqslant i<j\leqslant n}x_ix_j,\cdots,$$

$$a_s=\sum_{1<i_1<\cdots<i_s\leqslant n}x_{i_1}\cdots x_{i_s},\cdots,\quad a_n=x_1\cdots x_n$$

是$x_1,\cdots,x_n$的初等对称多项式；$F=k(a_1,\cdots,a_n)$。则K是F的

Galois 扩域，并且Galois 群 $G(K/F)$与 n 次对称群 S_n 同构。

证 $\{1,2,\cdots,n\}$的每一个置换 σ 唯一地确定K的一个k-自同构，仍以 σ 表示，使得

$$\sigma(x_i)=x_{\sigma(i)},\quad i=1,2,\cdots,n.$$

并且不同的置换所确定的自同构也不相同。令G是如上所给出的K的 k-自同构的全体。那么G是K的一切 k-自同构所成的群$G(K/k)$的一个子群，且$G\cong S_n$。令

$$F_0=K^G=\{a\in K\mid\sigma(a)=a,\ \forall\sigma\in G\}$$

是G的固定域。那么$k\subseteq F\subseteq F_0\subseteq K$。由3.3.2，$K/F_0$是Galois 扩张。它的 Galois 群就是$G$。所以$[K:F_0]=|G|=n!$。令

$$f(X)=\prod_{i=1}^{n}(X-x_i)=X^n-a_1X^{n-1}+$$
$$+a_2X^{n-2}-\cdots+(-1)^na_n.$$

则 $f(X)\in F[X]$。

我们有扩域序列

$$F\subseteq F(x_1)\subseteq F(x_1,x_2)\subseteq\cdots\subseteq F(x_1,\cdots,x_n)=K.$$

因为x_1是 $f(X)$的一个根，所以$[F(x_1):F]\leqslant\deg f=n$。其次，$x_2$ 是多项式 $f(X)/(X-x_1)\in F_1[X]$ 的一个根，这里 $F_1=$ $=F(x_1)$，所以

$$[F(x_1,x_2):F(x_1)]\leqslant\deg\frac{f(X)}{X-x_1}=n-1.$$

一般，对于 $1\leqslant s\leqslant n$，我们有

$$[F(x_1,\cdots,x_s):F(x_1,\cdots,x_{s-1})]\leqslant n-s+1,$$

所以$[K:F]\leqslant n!$。

另一方面，因为$F\subseteq F_0\subseteq K$，而$[K:F_0]=n!$，所以$[K:F]\geqslant n!$。这样一来，我们有$[K:F]=n!$，$F=F_0$，因此$K/F$ 是Galois扩张，它的 Galois 群与S_n同构。 ∎

现在设 k 是一个域，$t_1,\cdots,t_n$是 k 上 n 个不相关不定元。令

$F=k(t_1,\cdots,t_n)$。多项式

$$f(X)=X^n-t_1X^{n-1}+t_2X^{n-2}-\cdots+(-1)^nt_n\in F[X]$$

叫做 k 上 n 次一般多项式；相应地，方程 $f(X)=0$ 叫做 k 上 n 次一般方程.

定理 3.11.2 设 k 是一个域. k 上 n 次一般多项式

$$f(X)=X^n-t_1X^{n-1}+t_2X^{n-2}-\cdots+(-1)^nt_n$$

是 F 上一个可分的不可约多项式. $f(X)$ 在 F 上的 Galois 群与 n 次对称群 S_n 同构。

证 令 $\alpha_1,\cdots,\alpha_n$ 是 $f(X)$ 在 F 的某一个代数闭包内的全部根，$K=F(\alpha_1,\cdots,\alpha_n)$是 $f(X)$在 F 上的分裂域. 在 $K[X]$内，我们有

$$f(X)=(X-\alpha_1)\cdots(X-\alpha_n).$$

由根与系数的关系。我们有

$$t_1=\sum_{i=1}^n\alpha_i,\qquad t_2=\sum_{1\leqslant i<j\leqslant n}\alpha_i\alpha_j,\cdots,$$

$$t_s=\sum_{1\leqslant i_1<\cdots<i_s\leqslant n}\alpha_{i_1}\cdots\alpha_{i_s},\cdots,\quad t_n=\alpha_1\cdots\alpha_n.$$

而$K=F(\alpha_1,\cdots,\alpha_n)=k(t_1,\cdots,t_n,\alpha_1,\cdots,\alpha_n)=k(\alpha_1,\cdots,\alpha_n)$。

令 $\overline{K}=k(x_1,\cdots,x_n)$是 k 上 n 个不相关不定元 $x_1,\cdots,x_n$ 的有理分式域. 设

$$\bar{f}(X)=\prod_{i=1}^n(X-x_i)=X^n-a_1X^{n-1}+$$

$$+a_2X^{n-2}-\cdots+(-1)^na_n,$$

这里

$$a_1=\sum_{i=1}^nx_i,\ a_2=\sum_{1\leqslant i<j\leqslant n}x_ix_j,\cdots,a_n=x_1\cdots x_n,$$

令$\overline{F}=k(a_1,\cdots,a_n)\subseteq\overline{K}$. 由3.11.1，$\overline{K}/\overline{F}$是 $n!$ 次的 Galois 扩张，且$G(\overline{K}/\overline{F})\cong S_n$.

我们证明,存在K到$\overline{K}$的 k-同构$\varphi: K\to\overline{K}$,使得$\varphi(\alpha_i)=x_i$,

$1 \leqslant i \leqslant n$，如果这个断言被证明，那么就有$\varphi(t_i)=a_i$，$1 \leqslant i \leqslant n$，而$\varphi(F)=\bar{F}$。于是$K/F$是 Galois 扩张，并且$G(K/F) \cong S_n$。从而也就证明了$f(X)$在$F$上的 Galois 群与$S_n$同构，并且$f(X)$是$F$上一个可分的不可约多项式。

令$R=k[t_1, \cdots, t_n]$，$\bar{R}=k[a_1, \cdots, a_n] \subseteq k[x_1, \cdots, x_n]$。因为$t_1$，$\cdots$，$t_n$是$K$上不相关不定元，所以映射$\varphi: t_i \longmapsto a_i (1 \leqslant i \leqslant n)$可以自然地开拓为环$R$到环$\bar{R}$的满同态$\varphi: R \to \bar{R}$。设

$$h(t_1, \cdots, t_n) \in \operatorname{Ker}\varphi.$$

则

$$h(a_1, \cdots, a_n)=0.$$

于是$k[x_1, \cdots, x_n]$的元素

$$h(a_1(x_1, \cdots, x_n), \cdots, a_n(x_1, \cdots, x_n))=0,$$

这里

$$a_s(x_1, \cdots, x_n)=\sum_{1 \leqslant i_1<\cdots<i_s \leqslant n} x_{i_1} \cdots x_{i_s} \quad (1 \leqslant s \leqslant n).$$

另一方面，$\psi: k[x_1, \cdots, x_n] \to k[\alpha_1, \cdots \alpha_n]$，$\psi(x_i)=\alpha_i (1 \leqslant i \leqslant n)$，是环同态满射，而

$$\psi(a_s)=\psi(a_s(x_1, \cdots, x_n))=a_s(\alpha_1, \cdots, \alpha_n)=t_s (1 \leqslant s \leqslant n),$$

所以$h(a_1, \cdots, a_n)=0$，于是

$$h(t_1, \cdots, t_n)=\psi(h(a_1, \cdots, a_n))=0,$$

从而$\operatorname{Ker}\varphi=0$。这样$\varphi: R \to \bar{R}$是环同构映射。

φ可以唯一地开拓为R的商域$F=k(t_1, \cdots, t_n)$到$\bar{R}$的商域$\bar{F}=k(a_1, \cdots, a_n)$上的同构映射，因而可以唯一地开拓为多项式环$F[X]$到多项式环$\bar{F}[X]$上的同构映射$\varphi: F[X] \to \bar{F}[X]$。我们有

$$\varphi(f(X))=\bar{f}(X).$$

于是φ又可以开拓为$f(X)$在F上的分裂域K到$\bar{f}(X)$在$\bar{F}$上的分裂域$\bar{K}$上的同构映射。在这个开拓下，$\varphi(\alpha_i)=x_i (1 \leqslant i \leqslant n)$。定理被证明。 ∎

由这个定理，我们立即得到以下

定理 3.11.3 设 k 是一个特征为 0 的域，$t_1, \cdots, t_n$ 是 k 上不相关不定元，$F=k(t_1, \cdots, t_n)$. n 次一般方程

$$f(X)=X^n-t_1X^{n-1}+t_2X^{n-2}-\cdots+(-1)^nt_n=0$$

在 F 上可以用根号解的必要且充分条件是 $n\leqslant 4$.

证 $f(X)=0$ 在 F 上可以用根号解 $\Longleftrightarrow f(X)$ 的 Galois 群是可解群 $\Longleftrightarrow$ n 次对称群 S_n 是可解群 $\Longleftrightarrow n\leqslant 4$. ▮

由3.11.2，我们还得到以下

定理 3.11.4 给定一个有限群 G 和一个素数 p 或 0，那么存在一个特征为 p 或 0 的域 E 和 E 的一个 Galois 扩域 K，使得 $G(K/E)\cong G$.

证 设 G 的阶为 n，那么由Cayley定理，G 与 n 次对称群 S_n 的一个子群 H 同构. 令 k 是一个域. $\mathrm{char}k=p$ 或 0，$t_1, \cdots, t_n$ 是 k 上 n 个不相关不定元. 令 $F=k(t_1, \cdots, t_n)$. 取 K 是多项式

$$f(X)=X^n-t_1X^{n-1}+t_2X^{n-2}-\cdots+(-1)^nt_n\in F[X]$$

在 F 上的分裂域. 则 K 是 F 的 Galois 扩域，它的 Galois 群 $G(K/F)$ 与 S_n 同构. 对于 S_n 的子群 H，有 $G(K/F)$ 的一个与 H 同构的子群与它对应，仍记作 H. 令 E 是与 H 对应的 K/F 的中间域，则 K/E 是 Galois 扩张，且 $G(K/E)=H\cong G$. ▮

注意 一般，给定一个域 F 和一个有限群 G，是否存在 F 的一个 Galois 扩域 K，使得 K/F 的Galois群 $G(K/F)\cong G$. 这个问题的答案是否定的. 只要看一看有限域 F_q 或看实数域 $\mathbf{R}$ 或复数域 $\mathbf{C}$ 的情形就足以证明这一点. 当 $F=\mathbf{Q}$ 是有理数域时，除了个别的群 G 外，这个问题的一般解决也远没有得到.

最后我们讨论一下素数次方程.

引理 3.11.4 设 p 是一个素数，$f(X)$ 是某一个域 F 上 p 次可分多项式. 如果 $f(X)$ 的 Galois 群 G 不等于 S_p，则 $f(X)$ 在 F 上的分裂域可以由 $f(X)$ 的任意 p-2 个根生成.

证 设$\alpha_1,\cdots,\alpha_p$是$f(X)$在F的一个代数闭包内的全部根。$K=F(\alpha_1,\cdots,\alpha_p)$是$f(X)$在$F$上的分裂域。如果$f(X)$的某$p$-2个根不能生成$K$，那么对$f(X)$的根适当编号，可以假定$E=F(\alpha_3,\cdots,\alpha_p)\subsetneqq K$。$E$所对应的$G$的子群$H\neq\{1\}$。对于$\sigma=G$来说，$\sigma\in H\Longleftrightarrow\sigma(\alpha_j)=\alpha_j$，$j=3,\cdots,p$。所以对换$(12)\in H\subseteq G$。另一方面，因为$f(X)$在$F$上不可约。所以$[F(\alpha_1):F]=\deg f=p$，$F\subseteq F(\alpha_1)\subseteq K$，$G$中与$F(\alpha_1)$对应的子群的指数为$p$，所以$p\,|\,|G|$。因为$p$是一个素数，所以$G$含有一个$p$阶元素$\sigma$。作为$\{1,2,\cdots,p\}$的一个置换，$\sigma$是一个$p$-轮换。这样，$\sigma=(1i_2\cdots i_p)$，因此$\sigma$的若干次幂必有形状$\sigma^k=(12j_3,\cdots j_p)$，其中$\{j_3,\cdots,j_p\}=\{3,\cdots,p\}$。重新对$\alpha_3,\cdots,\alpha_p$编号（这不影响$E$），可设$\sigma^k=(12\cdots p)\in G$，又$G\ni(12)$，于是$G=S_p$。 ∎

定理 3.11.5 设F是实数域$\mathbf{R}$的一个子域，p是一个素数。如果F上p次不可约多项式$f(X)$恰有p-2个实根，则$f(X)$在F上的Galois群等于S_p。

证 设$\alpha_1,\cdots,\alpha_{p-2}$，$\alpha_{p-1}$，$\alpha_p\in\mathbf{C}$是$f(X)$的全部根，其中$\alpha_1,\cdots,\alpha_{p-2}$是实根而$\alpha_{p-1},\alpha_p$是一对非实的共轭复根。那么$f(X)$在$F$上的分裂域$K=F(\alpha_1,\cdots,\alpha_p)$不是实数域的子域。另一方面，$p$-2个实根$\alpha_1,\cdots\alpha_{p-2}$生成的子域$E=F(\alpha_1,\cdots,\alpha_{p-2})$是实数域$\mathbf{R}$的子域，因此$E\subsetneqq K$。于是由3.11.4，$f(X)$在$F$上的Galois群等于$S_p$。 ∎

例 设$f(X)=X^5-4X+2\in\mathbf{Q}[X]$。由Eisenstein判定法，$f(X)$在$\mathbf{Q}$上不可约。由方程论的知识可知$f(X)$恰有三个实根。所以$f(X)$的Galois群是$S_5$，因而方程$X^5-4X+2=0$在$\mathbf{Q}$上不能用根号解。

应该指出的是，一个代数方程能否用根号解是和基础域有关的。例如，方程$X^5-4X+2=0$在有理数域$\mathbf{Q}$上不能用根号解，然而在实数域$\mathbf{R}$上可以用根号解。事实上，$\mathbf{R}[X]$中每一个代数

方程在R上都可以用根号解，因为$C=R(\sqrt{-1})$就是R的一个根号扩域.

习　题

1. 令E是C的扩域，$E=C(t,u)$，其中t是C上不定元，u满足$C(t)$上方程$x^2+t^2=1$，确定$C(t,u)$在$C(t^{2m},u^{2m})$上的Galois群. 其中m是正整数.

3.12 二次、三次和四次方程

设k是一个特征为0的域. 我们给出k上二次、三次和四次一般方程的解.

二次方程的解　k上二次方程有形状

(1)　　$x^2-t_1x+t_2=0.$

令α_1，α_2是方程(1)在$F=k(t_1, t_2)$的一个代数闭包内的根，方程(1)的Galois群S_2由恒等置换及对换(α_1, α_2)构成，所以$(\alpha_1-\alpha_2)^2$在S_2的作用下保持不动，因而$(\alpha_1-\alpha_2)^2\in F$. 我们有

$$(\alpha_2-\alpha_1)^2=(\alpha_1+\alpha_2)^2-4\alpha_1\alpha_2=t_1^2-4t_2.$$

于是$\alpha_1-\alpha_2=\pm\sqrt{t_1^2-4t_2}$. 又$\alpha_1+\alpha_2=t_1$. 所以(1)的根的公式是

$$\alpha_1,\ \alpha_2=(t_1\pm\sqrt{t_1^2-4t_2})/2.$$

三次方程的解　k上三次一般方程有形状

(2)　　$x^3-t_1x^2+t_2x-t_3=0.$

通过未知量的代换

$$X=Y+\frac{1}{3}t_1,$$

方程(2)化为

(3)　　$Y^3+pY+q=0,$

p, $q \in F = k(t_1, t_2, t_3)$. 解(2)只需解(3). 设$\alpha_1, \alpha_2, \alpha_3$是方程(3)在$F$的某一个代数闭包内的全部根. 对称群$S_3$有合成列

$$S_3 \triangleright A_3 \triangleright (1).$$

先在基础域k内添加一个本原三次单位根ζ, $\zeta \neq 1$, $\zeta^3 = 1$. 令

$$\beta = \alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3,$$
$$\gamma = \alpha_1 + \zeta^2\alpha_2 + \zeta\alpha_3.$$

交错群A_3由3-轮换$(\alpha_1, \alpha_2, \alpha_3)$生成，所以使$\beta^3, \gamma^3$固定. 另一方面，$S_3$的任意对换都对调$\beta^3, \gamma^3$. 所以$\beta^3 + \gamma^3$, $\beta^3\gamma^3$在S_3的每一元素作用下保持不动，因而属于F. 我们有

$$\alpha_1 + \alpha_2 + \alpha_3 = 0,$$
$$\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = p,$$
$$\alpha_1\alpha_2\alpha_3 = -q.$$

由此得

$$\beta^3 + \gamma^3 = -27q$$
$$\beta^3\gamma^3 = -27p^3.$$

所以β^3, γ^3是二次多项式

(4) $$T^2 + 27qT - 27p^3$$

的根. 多项式(4)称为方程(3)的予解式. 由方程组

$$\alpha_1 + \zeta\alpha_2 + \zeta^2\alpha_3 = \beta,$$
$$\alpha_1 + \zeta^2\alpha_2 + \zeta\alpha_3 = \gamma.$$
$$\alpha_1 + \alpha_2 + \alpha_3 = 0$$

解出

$$\alpha_1 = \frac{1}{3}(\beta + \gamma),$$

$$\alpha_2 = \frac{1}{3}(\zeta\beta + \zeta^2\gamma),$$

$$\alpha_3 = \frac{1}{3}(\zeta^2\beta + \zeta\gamma).$$

通过简单的计算，我们有

$$\beta = \sqrt[3]{-27q/2 + (3\sqrt{3}/2)\sqrt{4p^3 + 27q^2}},$$

$$\gamma = \sqrt[3]{-27q/2 - (3\sqrt{3}/2)\sqrt{4p^3 + 27q^2}}.$$

四次方程的解 k 上四次方程

$$x^4 - t_1x^3 + t_2x^2 - t_3x + t_4 = 0$$

通过未知量的代换

$$X = Y + \frac{1}{4}t_1$$

可化为以下形式：

(5) $$Y^4 + pY^2 + qY + r = 0.$$

设$\alpha_1, \alpha_2, \alpha_3, \alpha_4$是方程(5)在域 $F = k(p, q, r)$ 的某一个代数闭包内的根，对称群S_4有合成列

$$S_4 \triangleright A_4 \triangleright V \triangleright \{1, (\alpha_1\alpha_2)(\alpha_3\alpha_4)\} \triangleright (1),$$

这里 $V = \{1, (\alpha_1\alpha_2)(\alpha_3\alpha_4), (\alpha_1\alpha_3)(\alpha_2\alpha_4), (\alpha_1\alpha_4)(\alpha_2\alpha_3)\}$. 令

$$\beta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4),$$

(6) $$\beta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4),$$

$$\beta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3).$$

则集$\{\beta_1, \beta_2, \beta_3\}$在$S_4$的所有置换之下不变. 所以 $\beta_1, \beta_2, \beta_3$ 的初等对称多项式属于F. 我们有

$$\beta_1 + \beta_2 + \beta_3 = 2p,$$

$$\beta_1\beta_2 + \beta_2\beta_3 + \beta_3\beta_1 = p^2 - 4r,$$

$$\beta_1\beta_2\beta_3 = -q^2.$$

$\beta_1\beta_2\beta_3$是F上三次多项式

$$T^3 - 2pT^2 + (p^2 - 4r)T + q^2$$

的根，这个三次多项式称为方程(5)的三次予解式. 因为$\alpha_1 + \alpha_2$

$+\alpha_3+\alpha_4=0$。所以由(6)，我们有

$$(\alpha_1+\alpha_2)^2=-\beta_1,$$
$$(\alpha_1+\alpha_3)^2=-\beta_2,$$
$$(\alpha_1+\alpha_4)^2=-\beta_3.$$

于是

$$2\alpha_1=\sqrt{-\beta_1}+\sqrt{-\beta_2}+\sqrt{-\beta_3},$$
$$2\alpha_2=\sqrt{-\beta_1}-\sqrt{-\beta_2}-\sqrt{-\beta_3},$$
$$2\alpha_3=\sqrt{-\beta_1}+\sqrt{-\beta_2}-\sqrt{-\beta_3},$$
$$2\alpha_4=-\sqrt{-\beta_1}-\sqrt{-\beta_2}+\sqrt{-\beta_3},$$

并且满足条件

$$\sqrt{-\beta_1}\sqrt{-\beta_2}\sqrt{-\beta_3}=-q.$$

第四章　超越扩张

在前面两章里，我们主要讨论了域的代数扩张．在这一章里，我们将一般地研究超越扩张（非代数扩张）．

4.1　超越基　超越次数

设 R 是一个有单位元 1 的交换环，S 是 R 的一个子环，并且 S 含有 R 的单位元，对于 $a_1, \cdots, a_n \in R$，令 $S[a_1, \cdots, a_n]$ 表示 $a_1, \cdots, a_n$ 在 S 上所生成的 R 的子环．

S 上 n 个不定元多项式环 $S[X_1, \cdots, X_n]$ 到 $S[a_1, \cdots, a_n]$ 的映射

$$\begin{aligned}\varphi: S[X_1, \cdots, X_n] \ni f(X_1, \cdots, X_n) = \\ \sum c_{i_1, \cdots, i_n} X_1^{i_1} \cdots X_n^{i_n} \longmapsto f(a_1, \cdots, a_n) = \\ \sum c_{i_1, \cdots, i_n} a_1^{i_1} \cdots a_n^{i_n} \in S[a_1, \cdots, a_n],\end{aligned}$$

$c_{i_1, \cdots, i_n} \in S$，是 $S[X_1, \cdots, X_n]$ 到 $S[a_1, \cdots, a_n]$ 的同态满射．

如果同态映射 φ 是单的，即 $S[X_1, \cdots, X_n] \cong S[a_1, \cdots, a_n]$，那么就说，$a_1, \cdots, a_n$ 在 S 上**代数无关**；如果 $a_1, \cdots, a_n \in R$ 不是在 S 上代数无关的，那么就说，$a_1, \cdots, a_n$ 在 S 上**代数相关**．

根据这个定义，对于 R 的元素 $a_1, \cdots, a_n$ 和 R 的子环 S 来说，

$a_1, \cdots, a_n$ 在 S 上代数无关

$\Longleftrightarrow \forall f \in S[X_1, \cdots, X_n]$，若 $f(a_1, \cdots, a_n) = 0$ 则 $f = 0$．

$\Longleftrightarrow S[a_1, \cdots, a_n]$ 中一切单项式 $a_1^{i_1} \cdots a_n^{i_n}$（$i_1, \cdots, i_n$ 是任意非负整数）的集在 S 上线性无关．

R 的元素 a 叫做子环 S 上一个**超越元**，如果 a 在 S 上代数无关；在相反的情形，就称 a 是 S 上一个**代数元**．

设 A 是环 R 的一个非空子集．如果 A 中任意有限元素都在 S

上代数无关，那么就说A在S上代数无关。空集($\varnothing\subseteq R$)被认为在S上代数无关。

由以上定义可以直接得出以下结论：

1. 环S上一个代数无关集的任意子集也在S上代数无关。

2. S上代数无关集里的任意元素都是S上超越元。

3. 设S'也是环R的子环且$S\subseteq S'$。如果R的子集A在S'上代数无关，那么A也在S上代数无关。

我们将引入域的超越基的概念，首先证明一个引理。

引理 4.1.1 设F是一个域，K是F的一个扩域，A和B是K的两个子集。对于A和B来说，以下三个条件是等价的：

(i) $A\cap B=\varnothing$且$A\cup B$在F上代数无关；

(ii) A在F上代数无关而B在$F(A)$上代数无关；

(iii) B在F上代数无关而A在$F(B)$上代数无关。

证 由于A与B的地位对称性，我们只需证(i)$\Longleftrightarrow$(ii)。

(i)$\Longrightarrow$(ii) $A\subseteq A\cup B$而$A\cup B$在F上代数无关，所以A在F上代数无关。我们证明B在$F(A)$上代数无关。

令$\eta_1,\cdots,\eta_m$是B中任意有限个元素，如果存在域$F(A)$上m个不定元$Y_1,\cdots,Y_m$的多项式

$$f(Y_1,\cdots,Y_m)=\sum_{(i)}c_{(i)}Y_1^{i_1}\cdots Y_m^{i_m},$$

$c_{(i)}=c_{i_1,\ldots,i_m}\in F(A)$，使得$f(\eta_1,\cdots,\eta_m)=0$，我们证明，所有系数$c_{(i)}=0$。$c_{(i)}\in F(A)$是$F$上关于$A$的元素的有理分式，因为只有有限个$c_{(i)}$，所以存在$\xi_1,\cdots,\xi_n\in A$和$u_{(i)}=u_{(i)}(X_1,\cdots,X_n)$，$v=v(X_1,\cdots,X_n)\in F[X_1,\cdots,X_n]$，且$v(\xi_1,\cdots,\xi_n)\neq 0$使得每一个$c_{(i)}$都可以表成

$$c_{(i)}=u_{(i)}(\xi_1,\cdots,\xi_n)/v(\xi_1,\cdots,\xi_n).$$

因为$f(\eta_1,\cdots,\eta_m)=\sum c_{(i)}\eta_1^{i_1}\cdots\eta_m^{i_m}=0$，所以

$$\sum_{(i)}v_{(i)}(\xi_1,\cdots,\xi_n)\eta_1^{i_1}\cdots\eta_m^{i_m}=0.$$

令

$$g=g(X_1,\cdots,X_n,Y_1,\cdots,Y_m)=$$
$$=\sum_{(i)}u_{(i)}(X_1,\cdots,X_n)Y_1^{i_1}\cdots Y_m^{i_m}.$$

g 是 F 上 $n+m$ 个不定元 $X_1,\cdots,X_n$，$Y_1,\cdots,Y_m$ 的多项式．我们有

$$g(\xi_1,\cdots,\xi_n,\eta_1,\cdots,\eta_m)=0.$$

因为 $A\cup B$ 在 F 上代数无关，且 $A\cap B=\varnothing$．$\xi_1,\cdots,\xi_n,\eta_1,\cdots$ $\cdots,\eta_m$ 是 $A\cup B$ 中互不相同的元素，因而在 F 上代数无关．所以 g 中系数必须全为零，由此得

$$u_{(i)}(X_1,\cdots,X_n)=0.$$

于是

$$c_{(i)}=u_{(i)}(\xi_1,\cdots,\xi_n)/v(\xi_1,\cdots,\xi_n)=0,$$

从而 $f(Y_1,\cdots,Y_m)=0$．这就证明了 B 在 $F(A)$ 上代数无关．

(ii)$\Longrightarrow$(i)　设 A 在 F 上代数无关，B 在 $F(A)$ 上代数无关．如果有 $c\in A\cap B$，那么 $f(X)=X-c\in F(A)[X]$ 而 $f(c)=0$．因而 $c\in B$ 是 $F(A)$ 上代数元．这与 B 在 $F(A)$ 上代数无关的假设矛盾．因此 $A\cap B=\varnothing$．

现在证明 $A\cup B$ 在 F 上代数无关．设 $\xi_1,\cdots,\xi_n,\eta_1,\cdots,\eta_m$ 是 $A\cup B$ 中任意 $n+m$ 个元素，其中 $\xi_1,\cdots,\xi_n\in A$，$\eta_1,\cdots,\eta_m\in B$，我们证明，如果有 F 上 $n+m$ 个不定元 $X_1,\cdots,X_n,Y_1,\cdots,Y_m$ 的多项式 $g(X_1,\cdots,X_n,Y_1,\cdots,Y_m)$，使得

$$g(\xi_1,\cdots,\xi_n,\eta_1,\cdots,\eta_m)=0,$$

则 $g=0$．

当 $n=0$ 或 $m=0$ 时，显然 $g=0$，因此 A 和 B 都在 F 上代数无关．

设 $n\geqslant 1$ 且 $m\geqslant 1$，将 g 写成多项式环 $F[X_1,\cdots,X_n]$ 上关于 $Y_1\cdots,Y_m$ 的多项式：

$$g=\sum_{(i)}u_{(i)}(X_1,\cdots,X_n)Y_1^{i_1}\cdots Y_m^{i_m},$$

$u_{(i)}(X_1,\cdots,X_n)=u_{i_1\cdots i_m}(X_1,\cdots,X_n)\in F[X_1,\cdots X_n]$。令

$$f(Y_1,\cdots,Y_m)=\sum_{(i)}u_{(i)}(\xi_1,\cdots,\xi_n)Y_1^{i_1}\cdots Y_m^{i_m},$$

则 $f(Y_1,\cdots,Y_m)\in F(A)[Y_1,\cdots,Y_m]$，因为$B$在$F(A)$上代数无关，所以

$$f(\eta_1,\cdots,\eta_m)=0\Longrightarrow u_{(i)}(\xi_1,\cdots,\xi_n)=0,\ \forall(i).$$

又因为$\xi_1,\cdots,\xi_n$在F上代数无关，所以$u_{(i)}(X_1,\cdots,X_n)=0$，$\forall(i)$。于是

$$g(X_1,\cdots,X_n,\ Y_1,\cdots,Y_m)=0.$$

所以$A\cup B$在F上代数无关。 ▮

设K是域F的一个扩域。K的一个子集B叫做K在F上一个**超越基**，如果下列两条件被满足：

1. B在F上代数无关；
2. K是$F(B)$的代数扩域。

如果存在K在F上超越基B，使得$K=F(B)$，那么就说K是F的一个**纯超越扩域**，而K/F称为一个**纯超越扩张**。

我们证明超越基的存在性（可能是空集）。为此，只需证明以下的

定理 4.1.2 设K是域F的一个扩域，A和C是K的子集，且$A\subseteq C$。A在F上代数无关而K是$F(C)$的代数扩域。那么存在K在F上的一个超越基B，$A\subseteq B\subseteq C$。

证 令$S=\{B'\subseteq K\mid A\subseteq B'\subseteq C, B'$在$F$上代数无关$\}$。显然$A\in S$，所以$S\neq\varnothing$。对于集合的包含关系来说，$S$作成一个偏序集。设$\{B_\lambda\mid\lambda\in\Lambda\}$是$S$中一个链（$\Lambda$是一个指标集）。令$B^*=$
$=\bigcup_{\lambda\in\Lambda}B_\lambda$。则$A\subseteq B^*\subseteq C$。设$\xi_1,\cdots,\xi_m$是$B^*$中任意有限个元素。那么存在某一个$B_\lambda$，$\lambda\in\Lambda$，使得$\xi_1,\cdots,\xi_m\in B_\lambda$。因为$B_\lambda$在$F$上代数无关，所以$\xi_1,\cdots,\xi_m$在$F$上代数无关，因而$B^*$在$F$上代数

无关，所以$B^*\in S$．显然对于任意$\lambda\in\Lambda$，$B^*\supseteq B_\lambda$．所以B^*是$\{B_\lambda|\lambda\in\Lambda\}$的一个上界．因此$S$是归纳集．于是由Zorn引理，$S$有一个极大元$B$．$A\subseteq B\subseteq C$．

我们证明，B就是K在F上一个超越基．首先，$B\in S$，所以B在F上代数无关．其次，我们有$F(B)\subseteq F(C)\subseteq K$，而$K$是$F(C)$的代数扩域．这样，我们只需证明$F(C)$是$F(B)$的代数扩域即可．如果有$\xi\in F(C)$而$\xi$是$F(B)$上超越元，那么集$\{\xi\}$在$F(B)$上代数无关，且$\xi\notin B$而$B$又在$F$上代数无关，于是由4.1.1，$B\cup\{\xi\}$在$F$上代数无关．我们有

$$A\subseteq B\cup\{\xi\}\subseteq C,$$

所以$B\cup\{\xi\}\in S$．然而$\xi\notin B$，所以$B\subsetneq B\cup\{\xi\}$，这与B是S的极大元的事实相矛盾．于是，C在$F(B)$上是代数的，从而$F(C)$是$F(B)$的代数扩域．这就证明了K是$F(B)$的代数扩域．B是K在F上一个超越基． ▮

推论 4.1.3 域F的任意一个扩域K都存在F上的超越基．

证 在4.1.2里，取$A=\varnothing$，$C=K$． ▮

推论 4.1.4 设F是一个域，K是对F添加一个集C所得的扩域，$K=F(C)$，那么一定存在K在F上一个超越基B，且$B\subseteq C$．

证 在4.1.2里，取$A=\varnothing$． ▮

域F的一个扩域K在F上的超越基并不是唯一的．自然发生这样的问题：给了K在F上两个超越基B和C．它们的基数是否相同？下面将对这个问题作出肯定的回答．

以下我们用$|B|$表示一个集B的基数．

先考虑一个简单的情形，即K在F上有一个超越基是有限集的情形．这时我们有

引理 4.1.5 设K是域F的一个扩域．如果K在F上有一个超越基B含有n个元素（n是一个非负整数），那么K在F上任意超越基都含有n个元素．

证 设B'是K在F上任意一个超越基。我们证明$|B'|\leqslant n\leqslant|B|$。由此，对调$B$与$B'$的地位，又有$|B|\leqslant|B'|$，从而$|B|=$
$=|B'|$。

当$n=0$时，$B=\varnothing$，这时K是F的代数扩域。所以K不含F上的超越元素，因而$|B'|=0$。

设$n>0$，假设对于任意域扩张L/M来说，只要有一个超越基B_1，而$|B_1|=k<n$，那么对于L/M的任意超越基B'_1，就有$|B'_1|\leqslant k$。

现在设B'是K在F上任意一个超越基。如果$B'\subseteq B$，那么自然有$|B'|\leqslant n$。设$B'\not\subseteq B$，那么存在$\xi\in B'$而$\xi\notin B$。集$\{\xi\}$在F上代数无关，又$F(B)\subseteq F(B\cup\{\xi\})\subseteq K$，而$K$是$F(B)$的代数扩域，所以$K$是$F(B\cup\{\xi\})$的代数扩域。由4.1.2，存在$K$在$F$上一个超越基$\bar{B}$，使得$\{\xi\}\subseteq\bar{B}\subseteq B\cup\{\xi\}$。记$\bar{B}=C\cup\{\xi\}$，则$C\subseteq B$。因为$K$是$F(B)$的代数扩域，所以$\xi$是$F(B)$上代数元。由4.1.1，$B\cup\{\xi\}$在$F$上不是代数无关的。然而$\bar{B}=C\cup\{\xi\}\subseteq B\cup\{\xi\}$，所以$C\subsetneqq B$。因此$|C|<|B|=n$。

令$F'=F(\xi)$。我们证明，C与$B''=B'\setminus\{\xi\}$都是K在F'上的超越基。

事实上，因为$\bar{B}=C\cup\{\xi\}$在F上代数无关，由4.1.1，C在$F'=F(\xi)$上代数无关。其次，$F'(C)=F(\bar{B})$，而K是$F(\bar{B})$上代数扩域，所以K是$F'(C)$上代数扩域。因此C是K在F'上一个超越基。

同理可证$B''=B'\setminus\{\xi\}$也是K在F'上一个超越基。

由于$|C|<n$。又由归纳法假设$|B''|\leqslant|C|$，所以$|B'|=|B''|+1\leqslant|C|+1\leqslant n$。引理被证明。 ▮

现在证明一般的

定理 4.1.6 设K是域F的一个扩域。K在F上任意两个超越基都有相同的基数。

证 设B和C是K/F的两个超越基。如果B与C之一是有限集，那么由4.1.5，另一个也是有限集，并且$|B|=|C|$。

现在设B与C都是无限集。

设$\gamma\in C$。因为B是K/F的超越基，所以γ是$F(B)$上代数元。因此γ是系数在$F(B)$内的某个多项式

$$f(X)=\sum_{i=0}^{m} c_i X^i, \qquad c_i\in F(B), c_m=1,$$

的根。存在$\xi_1,\cdots,\xi_l\in B$和多项式$u_i(X_1,\cdots,X_l), 1\leqslant i\leqslant m-1$, $v(X_1,\cdots,X_l)\in F[X_1,\cdots,X_l]$，$v(\xi_1,\cdots,\xi_l)\neq 0$使得，

$$c_i=u_i(\xi_1,\cdots,\xi_l)/v(\xi_1,\cdots,\xi_l),\ 1\leqslant i\leqslant m-1.$$

因此，$f(X)$是系数在$F(\xi_1\cdots,\xi_l)$内的多项式。令$B_\gamma=\{\xi_1,\cdots,\xi_l\}\subseteq B$，则$\gamma$是$F(B_\gamma)$上代数元。

这样，对于C的每一个元素γ，可以选取B的一个有限子集B_γ，使得γ是$F(B_\gamma)$上的代数元。

显然$\bigcup\limits_{\gamma\in C} B_\gamma\subseteq C$。假设存在$\beta\in B$而$\beta\notin\bigcup\limits_{\gamma\in C} B_\gamma$。由于$C$是$K/F$的超越基，所以$\beta$是$F(C)$上代数元。另一方面，$C$的每一个元素都是$F(\bigcup\limits_{\gamma\in C} B_\gamma)$上的代数元，所以$F(C)$是$F(\bigcup\limits_{\gamma\in C} B_\gamma)$的代数扩域。因此$\beta$是$F(\bigcup\limits_{\gamma\in C} B_\gamma)$上的代数元。然而$\beta\notin\bigcup\limits_{\gamma\in C} B_\gamma$，所以由4.1.1，$B$的子集$(\bigcup\limits_{\gamma\in C} B_\gamma)\cup\{\beta\}$在$F$上不是代数无关的，这与$B$是$K/F$的超越基的假设矛盾。这样就有$B=\bigcup\limits_{\gamma\in C} B_\gamma$。

因为C是无限集，而每一个B_γ都是有限集，所以我们有

$$|B|=\left|\bigcup_{\gamma\in C} B_\gamma\right|\leqslant\aleph_0\cdot|C|=|C|,$$

这里$\aleph_0$表示可数集的基数。

对调B与C的地位，我们又有$|C|\leqslant|B|$。因此$|B|=|C|$。▮

定理 4.1.6 表明，域扩张 K/F 的任意两个超越基都具有相同的基数.我们把这唯一确定的基数定义为**K在F上的超越次数**，记作$\mathrm{tr.deg}_F K$或$\mathrm{tr.deg}(K/F)$.

定理 4.1.7 设K是域F的一个扩域.

（i） K/F是代数扩张$\Longleftrightarrow \mathrm{tr.deg}_F K=0$.

（ii） 设K是对F添加n（$n\geqslant 0$）个元素$\alpha_1,\cdots,\alpha_n$所生成的：$K=F(\alpha_1,\cdots,\alpha_n)$. 那么$\mathrm{tr.deg}_F K\leqslant n$.

证 （i） K/F是代数扩张$\Longleftrightarrow K/F$的超越基是空集$\Longleftrightarrow$ $\mathrm{tr.deg}_F K=0$.

（ii） 由4.1.4，存在K/F的超越基B，使得$B\subseteq\{\alpha_1,\cdots,\alpha_n\}$. 所以$\mathrm{tr.deg}_F K\leqslant n$. ∎

定理 4.1.8 设K是域F的一个扩域，且$\mathrm{tr.deg}_F K=n$.

（i） K的子集A如果在F上代数无关，则$|A|\leqslant n$. $|A|=n\Longleftrightarrow A$是$K/F$的一个超越基.

（ii） 设C是K的一个子集而K是$F(C)$的代数扩域，则$|C|\geqslant n$. $|C|=n\Longleftrightarrow C$是$K/F$的一个超越基.

证 （i） 由4.1.2. 存在K/F的超越基B，使得$A\subseteq B$. 因此$|A|\leqslant|B|=n$. $|A|=n\Longleftrightarrow A=B$.

（ii） 如同（i）一样，由4.1.2存在K/F的超越基B使得$B\subseteq C$. 所以$n=|B|\leqslant|C|$. $|C|=n\Longleftrightarrow C=B$. ∎

定理 4.1.9 设$F\subseteq K\subseteq L$是一串扩域. 我们有

$$\mathrm{tr.deg}_F L=\mathrm{tr.deg}_K L+\mathrm{tr.deg}_F K.$$

证 设B是K/F的一个超越基，C是L/K的一个超越基. 我们证明，$B\cup C$是L/F的一个超越基，且$B\cap C=\varnothing$.

因为B在F上代数无关，C在K上代数无关，所以C在$F(B)$上代数无关. 由4.1.1，$B\cap C=\varnothing$，且$B\cup C$在F上代数无关. 为了证明$B\cup C$是L/F的一个超越基，只需证明L是$F(B\cup C)$上的代数扩域.

因为K是$F(B)$上的代数扩域，所以K的元素是$F(B\cup C)$上的代数元，因而域$K(B\cup C)=F(B\cup C)(K)$是$F(B\cup C)$上的代数扩域．另一方面，$K(C)\subseteq K(B\cup C)\subseteq L$，而$L$是$K(C)$上的代数扩域，所以也是$K(B\cup C)$上的代数扩域．于是$L$是$F(B\cup C)$上的代数扩域．这就证明了$B\cup C$是$L/F$的一个超越基．于是

$$\text{tr.deg}_F L=|B\cup C|=|B|+|C|=$$
$$\text{tr.deg}_F K+\text{tr.deg}_K L. \quad \blacksquare$$

推论 4.1.10 设L是域F的一个扩域，而K是L/F的一个中间域．那么$\text{tr.deg}_F K\leqslant\text{tr.deg}_F L$． ▮

定理 4.1.11 设M是域F的一个扩域，K和L都是M/F的中间域，KL是K与L的合成域．那么

$\text{tr.deg}_K KL\leqslant\text{tr.deg}_F L$；$\text{tr.deg}_L KL\leqslant\text{tr.deg}_F K$；

$\text{tr.deg}_F KL\leqslant\text{tr.deg}_F K+\text{tr.deg}_F L$．

证 令B是L/F的一个超越基．L的每一个元素都是$F(B)$上的代数元，所以$KL=K(L)$是$K(B)$上的代数扩域．由4.1.2，存在KL/K的一个超越基C，且$C\subseteq B$．于是

$$\text{tr.deg}_K KL=|C|\leqslant|B|=\text{tr.deg}_F L.$$

同理有

$$\text{tr.deg}_L KL\leqslant\text{tr.deg}_F K.$$

再由4.1.9，

$$\text{tr.deg}_F KL=\text{tr.deg}_F K+\text{tr.deg}_K KL$$
$$\leqslant\text{tr.deg}_F K+\text{tr.deg}_F L. \quad \blacksquare$$

在2.3里，我们定义域F的正规扩域E是满足是以下两个条件的一个扩域：

1. E是F的代数扩域；
2. E在F上的每一个共轭域都等于E．

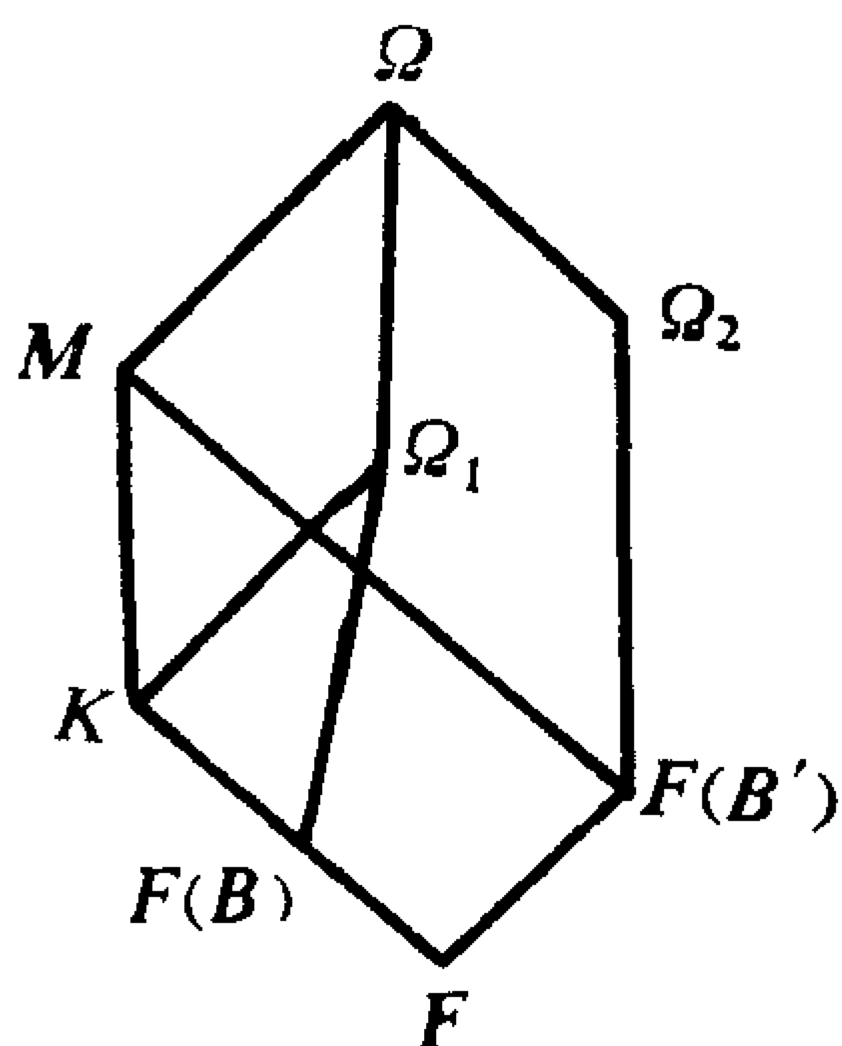
下面的定理表明，在正规扩域的定义里，条件1是多余的．

定理 4.1.12 设K是域F的一个扩域．如果K在F上每一

个共轭域都等于K本身，则K是F的代数扩域.

证 假设K是F的超越扩域. 我们证明，存在K的一个扩域Ω和一个K到Ω内的F-共轭$\sigma: K\to\Omega$，使得$\sigma(K)\neq K$.

令$B=\{\xi_\lambda\}_{\lambda\in\Lambda}$是$K/F$的一个超越基. 令$B'=\{X_\lambda\}_{\lambda\in\Lambda}$是与$B$具有同一指标集$\Lambda$的$K$上不相关不定元的集. 令$M=K(B')$是$K$上关于$B'=\{X_\lambda\}_{\lambda\in\Lambda}$的有理分式域（即$K$上关于$B'$的一切有限子集的有理分式域的并集）. 我们有$F\subseteq F(B)\subseteq K\subseteq M$.



令Ω是M的一个代数闭包，令Ω_1是$F(B)$在Ω内的代数闭包，Ω_2是$F(B')$在Ω内的代数闭包.

集$B=\{\xi_\lambda\}_{\lambda\in\Lambda}$在$F$上代数无关，所以存在$F$-同构

$$\varphi: F(B)\xrightarrow{\sim}F(B'),$$

$$\varphi(\xi_\lambda)=X_\lambda,\ \lambda\in\Lambda.$$

φ可以开拓为$F(B)$的代数闭包Ω_1到$F(B')$的代数闭包Ω_2的一个F-同构，仍用φ来表示这个开拓. 令$K'=\varphi(K)\subseteq\Omega_2$. 由$\{X_\lambda\}_{\lambda\in\Lambda}$的取法和$\varphi$的作法，我们有$\sigma=\varphi|_K: K\to\Omega$是$K$到$\Omega$的一个$F$-共轭. $X_\lambda=\varphi(\xi_\lambda)\in K'$但$X_\lambda\notin K$，所以$K'\neq K$. 这与题设相矛盾. ▮

习 题

1. 令K是域F的一个扩域，S是K的一个子集. 设$\alpha\in K$在$F(S)$上是代数的，而α在$F(S\setminus\{\beta\})$上不是代数的，其中$\beta\in S$. 证明，β在$F((S\setminus\{\alpha\})\cup\{\beta\})$上是代数的.

2. 设K是域F的一个扩域，A和C都是K的子集，其中A在F上代数无关而K是$F(C)$的代数扩域. 那么存在C的一个子集C'，使得$A\cap C'=\varnothing$且$B=A\cup C'$是K在F上一个超越基.

3. (i) 设B是复数域C在有理数域Q上一个超越基. 则B是无限集.

(ii) 证明，C有无限多个互不相同的自同构.

(iii) 证明，$\text{tr.deg}_Q C = |C|$.

4. 设F是一个代数闭域Ω的子域，K是Ω/F的一个中间域，且$\text{tr.deg}_F K$是有限的. 证明，K到Ω内的任意一个F-同态单射都可以开拓成为Ω的一个自同构.

5. 如果在习题4里，去掉$\text{tr.deg}_F K$是有限的条件，习题4的结论是否还成立？

6. 设$K = F(X_1, \cdots, X_n)$是域F上n个不定元的有理分式域，S_n和A_n分别是n次对称群和n次交错群. 对于$\sigma \in S_n$，$f(X_1, \cdots, X_n) \in K$，定义

$$\sigma(f(X_1, \cdots, X_n)) = f(X_{\sigma(1)}, \cdots, X_{\sigma(n)}).$$

则σ是K的一个自同构. 令

$$L = \{f \in K \mid \sigma(f) = f, \forall \sigma \in S_n\};$$

$$M = \{f \in K \mid \sigma(f) = f, \forall \sigma \in A_n\}.$$

证明，L和M都是F上超越次数为n的纯超越扩域.

4.2 Lüroth定理

一个域F上的纯超越扩域，特别是有限生成的纯超越扩域，看起来是比较简单的. 我们知道，F上任意一个有限生成的纯超越扩域K都与F上n个不定元$X_1, \cdots, X_n$的有理分式域$F(X_1, \cdots, X_n)$同构. 然而尽管如此，一般说来，一个纯超越扩张K/F的中间域是什么样子还不容易弄清楚. 在这一节里，我们将对于最简单的纯超越扩张，也就是超越次数是1的纯超越扩张，给出它的中间域的结构.

先证两个引理.

引理 4.2.1 设X和Y是域F上不相关不定元，$f(X)$，$g(X)$

是一对互素的多项式。那么多项式$g(X)Y-f(X)$是$F(Y)[X]$的不可约多项式。

证 $R=F[X]$是唯一因式分解整环，多项式$g(X)Y-f(X)$是$R[Y]$中的本原多项式，并且是R的商域$F(X)$上关于Y的一次多项式，因而是$R[Y]$的不可约的本原多项式。所以$g(X)Y-f(X)$是$R[Y]=F[X,Y]$中关于两个文字X,Y的不可约多项式，又因为$F[Y]$是唯一因式分解整环，所以$g(X)Y-f(X)$是$F[Y]$的商域$F(Y)$上关于X的不可约多项式。 ▮

引理 4.2.2 设F是一个域，$K=F(x)$，x是F上一个超越元；$u\in K$但$u\notin F$，$u=f(x)/g(x)$，其中$f(x),g(x)\in F[x]$是互素的多项式。那么K是$F(u)$上有限次扩域，并且

$$[K:F(u)]=\max(\deg f(x),\deg g(x)).$$

证 u是F上超越元（见2.1.9）。考虑$F(u)$上关于不定元T的多项式

$$\varphi(T)=g(T)u-f(T).$$

则$f(T)$，$g(T)\in F[T]$，且$(f(T),g(T))=1$。由4.2.1，$\varphi(T)$是$F(u)$上不可约多项式。我们有

$$\varphi(x)=g(x)u-f(x)=0.$$

所以x是$F(u)$上代数元，并且

$$[K:F(u)]=[F(x):F(u)]=\deg\varphi(T).$$

因为u是F上的超越元，所以在$\varphi(T)=g(T)u-f(T)$中，$g(T)u$与$f(T)$中关于T的同次项的系数不能互相抵消。于是

$$\deg\varphi(T)=\max(\deg f(T),\deg g(T)).$$ ▮

现在我们证明以下

定理 4.2.3 (Lüroth) 设$K=F(x)$是域F的一个纯超越扩域，E是K/F的一个中间域，且$E\neq F$。那么存在F上一个超越元t，使得$E=F(t)$。

证 因为$F\subsetneq E$，所以存在$u\in E$，但$u\notin F$。由4.2.2，K是

$F(u)$的有限次扩域，因而是E的有限次扩域，所以K是E的代数扩域，令$x\in K$在E上的最小多项式是

$$f_0(T)=T^n+a_1T^{n-1}+\cdots+a_n.$$

$a_i\in E\subseteq K$. 每一个a_i都是F上关于x的有理分式，因此总可以表示成

$$a_i=a_i(x)=\frac{b_i(x)}{b_0(x)},$$

这里$b_i(x),b_0(x)\in F[x],1\leqslant i\leqslant n$，且$b_0(x),b_1(x),\cdots,b_n(x)$是$F[x]$中一组互素的多项式。于是

$$f(x,T)=b_0(x)T^n+b_1(x)T^{n-1}+\cdots+b_n(x)\in F[x,T].$$

$f(x,T)$关于T的次数是n. 又设$f(x,T)$关于x的次数是m.

因为x是F上的超越元，所以$a_1,\cdots,a_n$中至少有某一个a_i不属于F. 我们将这个a_i记作t. $t=a_i\notin F$.则t是F上超越元（2.1.9）. 现在证明，$E=F(t)$.

将$t=b_i(x)/b_0(x)$表示成$F[x]$中两个互素多项式的商：

$$t=g(x)/h(x),g(x),h(x)\in F[x],(g(x),h(x))=1,$$

且$g(x)\mid b_i(x),h(x)\mid b_0(x)$，于是$\deg g(x)\leqslant m$，$\deg h(x)\leqslant m$.

考虑$E[T]$的多项式

$$g(T)-th(T)=g(T)-\frac{g(x)}{h(x)}h(T).$$

那么x是这个多项式的一个根. 因此，在$E[T]$内，$f_0(T)$整除$g(T)-th(T)$. 所以

$$g(T)-th(T)=f_0(T)q_0(T),\quad q_0(T)\in E[T].$$

两边乘上$F[x]$的一个适当的多项式，我们可以得到

$$\varphi(x)(g(T)h(x)-g(x)h(T))=f(x,T)q_0(x,T).$$

$\varphi(x)\in F[x],q_0(x,T)\in F[x,T]$. 因为$f(x,T)$没有$F[x]$中次数大于零的因式，所以在$F[x,T]$里，$\varphi(x)$整除$q_0(x,T)$. 因此，存在$q(x,T)\in F[x,T]$，使得

$$g(T)h(x)-g(x)h(T)=f(x,T)q(x,T).$$

等式左端关于 x 的次数至多为 m，而右端 $f(x,T)$ 关于 x 的次数等于 m，因此只可能左端关于 x 的次数等于 m 并且右端 $q(x,T)$ 关于 x 的次数等于 0．所以 $q(x,T)=q(T)\in F[T]$.

我们证明，$q(T)=c\in F$．假设 $\deg q(T)>0$．令 α 是 $q(T)$ 的一个根（在 $F(x)$ 的一个代数闭包内）．于是就有

$$g(\alpha)h(x)-g(x)h(\alpha)=f(x,0)q(\alpha)=0.$$

如果 $g(\alpha)=h(\alpha)=0$，那么 $g(x)$ 与 $h(x)$ 可以同时被 α 在 F 上的最小多项式整除，这与 $g(x),h(x)$ 互素的假设矛盾．如果 $h(\alpha)\neq 0$，那么由上面的等式得出 $t=g(x)/h(x)=g(\alpha)/h(\alpha)$ 是 F 上代数元，这又导致矛盾，如果 $g(\alpha)\neq 0$，我们又得到 $t^{-1}=h(\alpha)/g(\alpha)$，也同样导致矛盾．这样一来，只能是 $q(T)=c\in F$．于是

$$g(T)h(x)-g(x)h(T)=cf(x,T),\quad c\in F.$$

由左端的多项式的形状可以看出，它关于 x 的次数与关于 T 的次数是相同的，都等于 m，而右端关于 T 的次数是 n．因此 $m=n$.

另一方面，因为 $t\in E$，所以 $F(t)\subseteq E\subseteq K$．于是

$$[K:F(t)]\geqslant[K:E]=n=m.$$

再由4.2.2，$[K:F(t)]=\max(\deg g(x),\deg h(x))\leqslant m$. 这样一来，就必须 $[K:F(t)]=[K:E]$，从而 $E=F(t)$．定理被证明． ∎

习　题

1. 设 F 是一个域，$K=F(x)$，x 是 F 上一个超越元．证明：

（i）对于 $y\in K$ 来说，$F(y)=F(x)$ 必要且只要

$$y=\frac{ax+b}{cx+d},$$

$a,b,c,d\in F$ 且 $ad-bc\neq 0$．

（ii） K的F-自同构群与F上二阶射影线性群$PSL_2(F)$同构，这里$PSL_2(F)$定义为F上全体二阶可逆方阵对方阵的乘法所成的群对其中心的商群．

2. 设F是一个域，$K=F(x,y)$，其中x是F上的超越元且$x^2+y^2=1$，证明K是F上的纯超越扩域．

3. 设F是一个域，$\mathrm{char}F\neq 2$．$K=F(x,y)$，其中x,y满足关系$ax^2+by^2=1$，$a,b\in F$且$ab\neq 0$．证明以下两个条件等价：

（i） 存在$t\in K$，使得$K=F(t)$；

（ii） 方程$aX^2+bY^2=Z^2$在F中有一个非零解．

4. 设F是一个无限域，$x_1,\cdots,x_n$是F上一组代数无关的元素，而K是$F(x_1,\cdots,x_n)/F$的一个中间域．又设$\mathrm{tr.deg}_F K=r$．证明，存在$y_1,\cdots,y_r$，使得$K\subseteq F(y_1,\cdots,y_r)$．

[提示：先设$r=1$，对n作归纳法，然后再对r作归纳法．]

5. 设F是一个特征不为3的域，x是F上一个超越元，$K=F(x,y)$，且$x^3+y^3=1$．证明，K不是F上纯超越扩张．

4.3 线性无缘

为了以下的讨论，在这一节里我们介绍域线性无缘的概念．先证明以下的

引理 4.3.1 设M是域F的一个扩域．K和L都是M/F的中间域．以下两个条件是等价的：

（i） K中任意一个在F上线性无关的子集也在L上线性无关；

（ii） L中任意一个在F上线性无关的子集也在K上线性无关．

证 （i）$\Longrightarrow$（ii） 令S是L的一个在F上线性无关的子集．$\beta_1,\cdots,\beta_m$是S中任意有限个元素．则$\beta_1,\cdots,\beta_m$在F上线性无关．如果有$\alpha_1,\cdots,\alpha_m\in K$，使得

$$a_1\beta_1+\cdots+a_m\beta_m=0,$$

适当编号，可设 $a_1,\cdots,a_n(n\leqslant m)$ 在 F 上线性无关，而每一个 a_i $(1\leqslant i\leqslant m)$ 可以表示成 $a_1,\cdots,a_n$ 的 F-线性组合：

$$a_i=\sum_{i=0}^{n}a_{ij}a_j,\quad a_{ij}\in F,$$

于是

$$0=\sum_{i=1}^{m}a_i\beta_i=\sum_{j=1}^{n}\left(\sum_{i=1}^{m}a_{ij}\beta_i\right)a_j=\sum_{j=1}^{n}\gamma_j a_j,$$

$\gamma_j=\sum_{i=1}^{m}a_{ij}\beta_i\in L(1\leqslant j\leqslant n)$。由(i)，我们有 $\gamma_j=0\ (1\leqslant j\leqslant n)$。从而 $a_{ij}=0\ (1\leqslant i\leqslant m,1\leqslant j\leqslant n)$。所以 $a_i=0\ (1\leqslant i\leqslant m)$。这样，$\beta_1,\cdots,\beta_m$ 在 L 上线性无关，即 S 在 L 上线性无关。

(ii)$\Longrightarrow$(i)　证明完全类似。 ▮

设 F 是一个域，M 是 F 的一个扩域，K 和 L 是 M/F 的中间域。如果引理中等价的两个条件之一被满足，那么就说 K 与 L 在 F 上**线性无缘**。

由定义直接得到以下

定理 4.3.2　设 M 是域 F 的一个扩域，K 和 L 是 M/F 的中间域。以下条件是等价的：

(i)　K 与 L 在 F 上线性无缘；

(ii)　K/F 的任意中间域 K' 与 L/F 的任意中间域 L' 在 F 上线性无缘；

(iii)　K 的任意在 F 上有限生成的子域 K' 与 L 的任意在 F 上有限生成的子域 L' 在 F 上线性无缘；

(iv)　对于 K 中任意在 F 上线性无关的元素 $a_1,\cdots,a_m$ 和 L 中任意在 F 上线性无关的元素 $\beta_1,\cdots,\beta_n$，乘积 $a_i\beta_j,1\leqslant i\leqslant m,1\leqslant j\leqslant n$，也在 F 上线性无关。

证　(i)$\Longrightarrow$(ii)，(ii)$\Longrightarrow$(iii)都是明显的。

(iii)$\Longrightarrow$(iv)　令 $K'=F(a_1,\cdots,a_m)$，$L'=F(\beta'_1,\cdots,\beta_n)$，

则K'与L'在F上线性无缘．如果有F上线性关系

$$\sum_{i=1}^{m}\sum_{j=1}^{n}a_{ij}\alpha_i\beta_j=0, a_{ij}\in F,$$

成立，那么由于$\beta_1,\cdots,\beta_m$在K上线性无关，而$\sum_{i=1}^{m}a_{ij}\alpha_i\in K$，所以$\sum_{i=1}^{m}a_{ij}\alpha_i=0$ $(1\leqslant i\leqslant m)$．又因为$\alpha_1,\cdots,\alpha_m$在$F$上线性无关，所以$a_{ij}=0$ $(1\leqslant i\leqslant m,\ 1\leqslant j\leqslant n)$．

(iv)$\Longrightarrow$(i) 设$S\subseteq K$是任意一个在F上线性无关的子集．令$\alpha_1,\cdots,\alpha_m$是S中任意有限个元素．如果有$\beta_1,\cdots,\beta_m\in L$，使得$\sum_{i=1}^{m}\alpha_i\beta_i=0$，适当编号，可以设$\beta_1,\cdots,\beta_n(n\leqslant m)$在$F$上线性无关，而每一$\beta_i(1\leqslant i\leqslant m)$可以由$\beta_1,\cdots,\beta_n$线性表示：

$$\beta_i=\sum_{j=1}^{n}a_{ij}\beta_j(1\leqslant i\leqslant m).$$

于是

$$\sum_{i=1}^{m}\sum_{j=1}^{n}a_{ij}\alpha_i\beta_j=0.$$

由(iv)，必须$a_{ij}=0, 1\leqslant i\leqslant m,\ 1\leqslant j\leqslant n$．因而$K$与$L$在$F$上线性无缘． ▮

定理 4.3.3 设K和L都是域扩张M/F的中间域，R是K的一个包含F的子整环，且K是R的商域．令$\{\omega_i\}_{i\in I}$是向量空间R在F上的一个基．那么K与L在F上线性无缘当且仅当$\{\omega_i\}_{i\in I}$在L上线性无关．

证 如果K与L在F上线性无缘，那么由4.3.1，$\{\omega_i\}_{i\in I}$在L上线性无关．

反之，设$\beta_1,\cdots,\beta_m$是L中任意有限个在F上线性无关的元素．假设存在$\alpha_1,\cdots,\alpha_m\in K$，使得$\sum_{i=1}^{m}\alpha_i\beta_i=0$．因为$K$是$R$的商域，我们可以用各$\alpha_i(1\leqslant i\leqslant m)$的公分母去乘这个等式两端而得到等式

$$\sum_{i=1}^{m} \xi_i\beta_i = 0\ ,\ \ \xi_i \in R.$$

因为$\{\omega_i\}_{i\in I}$是R在F上的一个基，所以存在有限个元素$\omega_1, \cdots, \omega_n \in \{\omega_i\}_{i\in I}$，使得

$$\xi_i = \sum_{j=1}^{n} a_{ij}\omega_j,\ \ a_{ij} \in F.$$

于是

$$\sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}\omega_j\beta_i = 0\ .$$

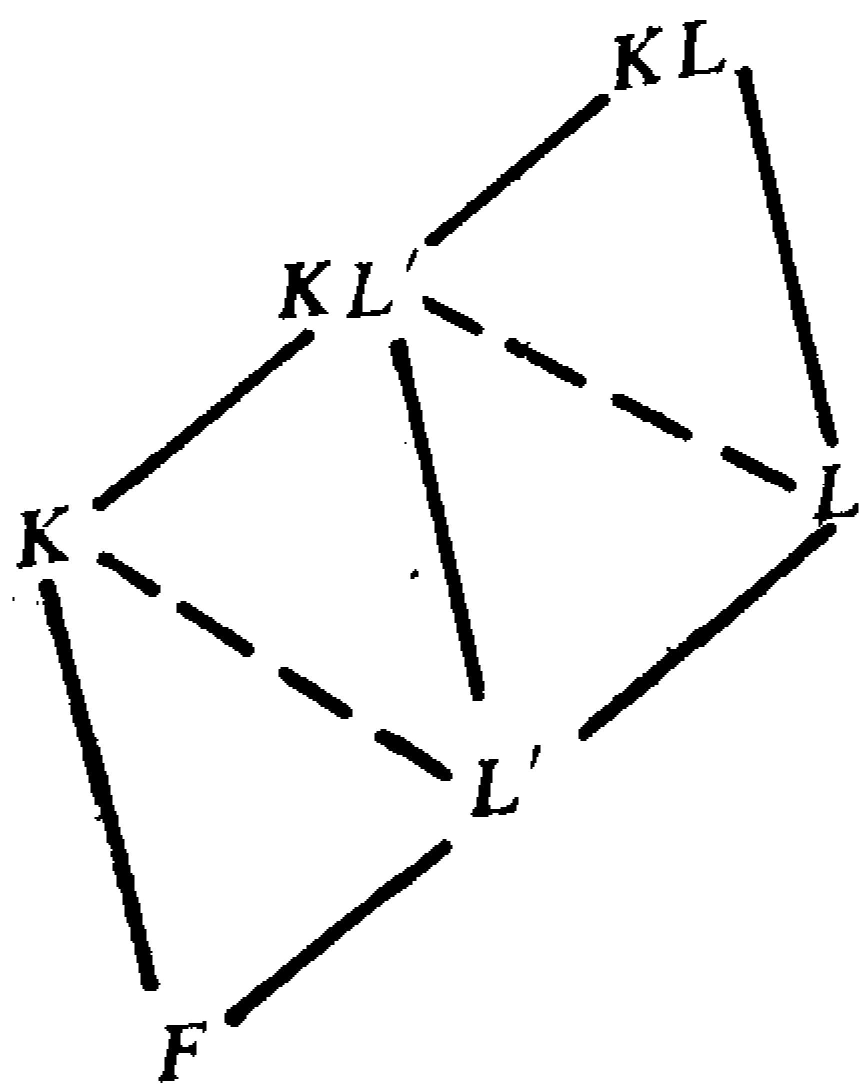
因为$\{\omega_i\}_{i\in I}$在L上线性无关，所以$\sum_{i=1}^{m} a_{ij}\beta_i = 0$，$1\leqslant j\leqslant n$。而$a_{ij} = 0\,(1\leqslant i\leqslant m,\ 1\leqslant j\leqslant n)$。由此得出$\alpha_i = 0\,(1\leqslant i\leqslant m)$。这就证明了$K$与$L$在$F$上线性无缘。 ▮

推论 4.3.4 设K和L都是域扩张M/F的中间域，$\{\omega_i\}_{i\in I}$是K在F上一个基。那么K与L在F上线性无缘当且仅当$\{\omega_i\}_{i\in I}$在L上线性无关。 ▮

定理 4.3.5 设K和L都是域扩张M/F的中间域，而L'是L/F的一个中间域。那么K与L在F上线性无缘当且仅当以下两条件成立：

(i) K与L'在F上线性无缘；

(ii) KL'与L在L'上线性无缘。



证 假设条件(i)和(ii)成立。设$\{\omega_i\}_{i\in I}$是K在F上一个基。因为K与L'在F上线性无缘，所以$\{\omega_i\}_{i\in I}$在L'上线性无关；又因为KL'与L在L'上线性无缘，所以$\{\omega_i\}_{i\in I}(\subseteq KL')$在$L$上线性无关。

于是由4.3.4，K与L在F上线性无缘。

反过来，设K与L在F上线性无缘。这时条件(i)自然成立，因为$L'\subseteq L$。令$\{\omega_i\}_{i\in I}$是K在F上一个基，那么$\{\omega_i\}_{i\in I}$在L上线性无关，所以在L'上线性无关。令

$$R=\{\sum_{i\in I}\beta_i\omega_i\ (\text{有限和})\mid\beta_i\in L'\}$$

R是L'上一个向量空间且$\{\omega_i\}_{i\in I}$是R在L'上一个基。然而另一方面，容易看出

$$R=\{\sum_{i\in I}\alpha_i\beta_i\ (\text{有限和})\mid\alpha_i\in K,\beta_i\in L'\}.$$

是KL'的一个子整环，并且KL'的元素都可以表示成ξ/η的形式，$\xi,\eta\in R,\eta\neq 0$。因此KL'是R的商域，于是由4.3.3，KL'与L在L'上线性无缘。 ∎

习　题

1. 设K和L都是域扩张M/F的中间域，并且$[K:F]<\infty$。证明：

（i） KL/L是有限次扩张，并且$[KL:L]\leqslant[K:F]$；

（ii） $[KL:L]=[K:F]$必要且只要K与L在F上线性无缘。

2. 设K和L都是域扩张M/F的中间域。证明：

（i） $[KL:F]<\infty\Longleftrightarrow[K:F]<\infty$且$[L:F]<\infty$；

（ii） 如果$[KL:F]<\infty$，则$[KL:F]\leqslant[K:F][L:F]$；

（iii） 如果$[K:F]$与$[L:F]$互素，则$[KL:F]=[K:F][L:F]$，并且这时K与L在F上线性无缘。

3. 设K和L都是域扩张M/F的中间域，并且K/F是有限次Galois扩张。证明，K与L在$K\cap L$上线性无缘。如果K/F和L/F都不是Galois扩张，上述断言是否仍成立？

4. 设K和L都是域扩张M/F的中间域，其中K/F是纯超越扩张而L/F是代数扩张。证明，K与L在F上线性无缘。

4.4 域的代数无关性

设F是一个域，M是F的一个扩域．在这一节里，我们将讨论域扩张M/F的两个中间域在F上的代数无关性．这是一个与线性无缘性既有区别又有联系的概念．

为了简单起见，我们把M中的n个元素$v_1,\cdots,v_n$所成的序组$(v_1,\cdots,v_n)$简记作(v)．设K是M的一个子域．对K添加M的元素$v_1,\cdots,v_n$所得的扩域$K(v_1,\cdots,v_n)$简记作$K(v)$．

引理 4.4.1 设M是域F的一个扩域．K和L是M/F的中间域．以下两个条件是等价的：

（i） K的任意一个在F上代数无关的子集也在L上代数无关；

（ii） L的任意一个在F上代数无关的子集也在K上代数无关．

证 （i）$\Longrightarrow$（ii） 设S是L的一个在F上代数无关的子集．令$v_1,\cdots,v_n$是S的任意有限个元素．我们证明，$v_1,\cdots,v_n$在K上代数无关．

记$F(v)=F(v_1,\cdots,v_n)$．因为$v_1,\cdots,v_n$在F上代数无关，所以$\mathrm{tr.deg}_F F(v)=n$．

如果$v_1,\cdots,v_n$在K上代数相关，那么存在一个非零多项式$f(X_1,\cdots,X_n)\in K[X_1,\cdots,X_n]$，使得$f(v_1,\cdots,v_n)=0$．令$\{a_1,\cdots,a_m\}$是$f(X_1,\cdots,X_n)$的系数所成的集．那么$K'=F(a_1,\cdots,a_m)\subseteq K$是$F$上有限生成的扩域，且$f(X_1,\cdots,X_n)\in K'[X_1,\cdots,X_n]$．所以$v_1,\cdots,v_n$在$K'$上代数相关．于是

$$\mathrm{tr.deg}_{K'} K'(v)<n.$$

设 $r=\mathrm{tr.deg}_F K'$，而$B'=\{y_1,\cdots,y_r\}$是K'在F上一个超越基．因为B'在F上代数无关，所以由（i），B'也在$F(v)$（$\subseteq L$）上代数无关．注意到$K'(v)=K'F(v)$，于是

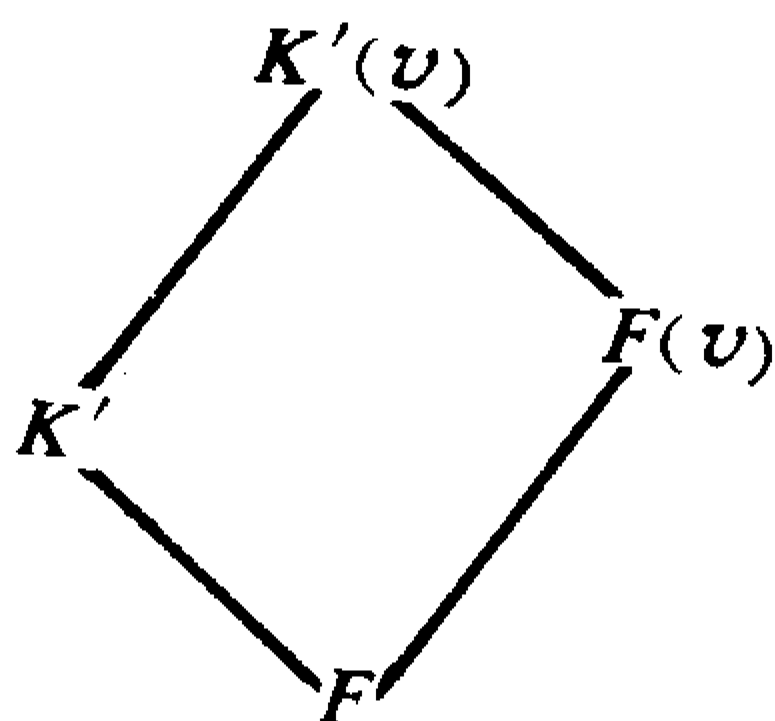
$$\mathrm{tr.deg}_F K' = r \leqslant \mathrm{tr.deg}_{F(v)} K'(v).$$

然而由4.1.11，我们有

$$\mathrm{tr.deg}_{F(v)} K'(v) \leqslant \mathrm{tr.deg}_F K' = r.$$

所以

$$\mathrm{tr.deg}_{F(v)} K'(v) = r.$$



由以上结果，按两种方法计算 $\mathrm{tr.deg}_F K'(v)$。一方面，

$$\mathrm{tr.deg}_F K'(v) = \mathrm{tr.deg}_{K'} K'(v) + \mathrm{tr.deg}_F K' < n + r;$$

另一方面，

$$\mathrm{tr.deg}_F K'(v) = \mathrm{tr.deg}_{F(v)} K'(v) + \mathrm{tr.deg}_F F(v) = r + n.$$

这就导致矛盾。因此 $v_1, \cdots, v_n$在K上代数无关。

(ii)⟹(i) 同样地证明。 ▮

设K和L是域扩张M/F的两个中间域。如果4.4.1中两个等价的条件之一被满足，那么就说**K与L在F上代数无关**。

定理 4.4.2 设K和L都是域扩张M/F的中间域。如果K与L在F上线性无缘，则K与L在F上代数无关。

证 我们证明，K中任意有限个在F上代数无关的元素也在L上代数无关。假设存在$u_1, \cdots, u_n \in K$，它们在F上代数无关而在L上代数相关，那么存在L上多项式

$$f(X_1, \cdots, X_n) = \sum_{(i)} c_{(i)} X_1^{i_1} \cdots X_n^{i_n} \neq 0,$$

$c_{(i)} = c_{i_1, \cdots, i_n} \in L$，使得$f(u_1, \cdots, u_n) = 0$。因此，出现在这个多项式中的所有单项式

$$\{M_{(i)}(u) = u_1^{i_1} \cdots u_n^{i_n}\} \subseteq K$$

在L上线性相关。由假设，K与L在F上线性无缘，所以这一组单项式$\{M_{(i)}(u)\}$在F上线性相关。于是存在一个线性关系

$$\sum a_{(i)} M_{(i)}(u) = 0,$$

$a_{(i)} \in F$，并且不全为零．令

$$h(X_1, \cdots, X_n) = \sum a_{(i)} X_1^{i_1} \cdots X_n^{i_n} \in F[X_1, \cdots, X_n].$$

则 $h(X_1, \cdots, X_n) \neq 0$，而 $h(u_1, \cdots, u_n) = 0$，这与 $u_1, \cdots, u_n$ 在 F 上代数无关的假设矛盾． ∎

定理 4.4.3 设 K 是域扩张 M/F 的中间域．令 $(u) = (u_1, \cdots, u_n)$ 是 M 中一组在 K 上代数无关的元素．那么 K 与 $F(u) = F(u_1, \cdots, u_n)$ 在 F 上线性无缘．

证 因为 $u_1, \cdots, u_n$ 在 K 上代数无关，所以也在 F 上代数无关．因此，作为 F 上的向量空间，一切单项式所成的集

$$\{u_1^{i_1} \cdots u_n^{i_n} \mid i_1, \cdots, i_n \in \mathbf{Z}_+\}$$

作成整环 $F[u] = F[u_1, \cdots, u_n]$ 在 F 上的一个基，这里 $\mathbf{Z}_+$ 表示全体非负整数集．

因为 $u_1, \cdots, u_n$ 在 K 上代数无关，所以 $u_1, \cdots, u_n$ 的任意有限个单项式在 K 上线性无关，所以 $F[u]$ 的基 $\{u_1^{i_1} \cdots u_n^{i_n} \mid i_1, \cdots, i_n \in \mathbf{Z}_+\}$ 在 K 上线性无关．于是由4.3.3，K 与 $F(u)$ 在 F 上线性无缘． ∎

定理 4.4.4 设 L 是域 F 上一个有限生成的扩域．那么 L/F 的任意中间域也是 F 上有限生成的．

证 设 K 是域扩张 L/F 的一个中间域．我们区别两个情形来考虑．

情形 1 K 是 F 的代数扩域．

设 $L = F(u_1, \cdots, u_n)$．适当编号，可以假设 $u_1, \cdots, u_s$ 是 L/F 的一个超越基．令 $E = F(u_1, \cdots, u_s)$．则 $L = E(u_{s+1}, \cdots, u_n)$ 是 E 的代数扩域．所以 L 是 E 的有限次扩域．

考虑合成域 $KE = K(u_1, \cdots, u_s) = E(K)$．因为 K 是 F 的代数扩域，所以 K 的每一个元素都是 E 上的代数元，因此 KE 是 E 的代数扩域．于是

$$\mathrm{tr.deg}_F KE = \mathrm{tr.deg}_E KE + \mathrm{tr.deg}_F E = s.$$

另一方面,

$$\mathrm{tr.deg}_F KE = \mathrm{tr.deg}_K KE + \mathrm{tr.deg}_F K = \mathrm{tr.deg}_K KE.$$

所以 $\mathrm{tr.deg}_K KE = s$. 于是由 4.1.8, $u_1, \cdots, u_s$ 在 K 上代数无关. 再由 4.4.3, K 与 E 在 F 上线性无缘. 这样一来, 如果 $\alpha_1, \cdots, \alpha_t$ 是 K 在 F 上任意一组线性无关的元素, 那么 $\alpha_1, \cdots, \alpha_t$ 也在 E 上线性无关, 所以 $t \leqslant [L : E]$. 因此

$$[K : F] \leqslant [L : E] < \infty.$$

所以 K 是 F 的有限次扩域, 因而是 F 上有限生成的扩域.

情形 2 K 不是 F 的代数扩域. 我们有

$$\mathrm{tr.deg}_F K \leqslant \mathrm{tr.deg}_F L < \infty.$$

令 $r = \mathrm{tr.deg}_F K$, 而 $u_1, \cdots, u_r$ 是 K 在 F 上一个超越基. 令 $F' = F(u_1, \cdots, u_r)$. 那么 K 是 F' 的代数扩域. 又 L 是 $F'(\supseteq F)$ 上有限生成的, 于是由情形 1, K 是 F' 上有限生成的. 因此, 存在 $v_1, \cdots, v_s \in K$, 使得 $K = F'(u_1, \cdots, u_s)$, 从而 $K = F(u_1, \cdots, u_r, v_1, \cdots, v_s)$ 是 F 上有限生成的. ∎

习　题

1. 设 K 是域扩张 M/F 的一个中间域. $u_1, \cdots, u_n \in M$. 记 $(u) = (u_1, \cdots, u_n)$. 证明

$$\mathrm{tr.deg}_K K(u) \leqslant \mathrm{tr.deg}_F F(u).$$

当且仅当 K 与 $F(u)$ 在 F 上代数无关时, 等号成立.

2. 设复数 t 是有理数域 $\mathbf{Q}$ 上一个超越元.

$E = \mathbf{Q}(t), F = \mathbf{Q}(t+i)\ (i = \sqrt{-1})$. 证明:

(i) $E \cap F = \mathbf{Q}$;

(ii) E 与 F 在 $\mathbf{Q}$ 上不是代数无关的.

4.5 可分扩张

在第二章里，我们已经介绍了可分和不可分域扩张的概念．那时说到可分或不可分域扩张，都指的是代数扩域．现在我们将推广这个概念，讨论一般的可分扩张．

首先给出可分代数扩张的一个等价的定义．

引理 4.5.1 设 F 是一个特征为 $p>0$ 的域，K 是 F 的一个代数扩域．Ω 是 K 的一个代数闭包．令 $F^{1/p}=\{\alpha\in\Omega\mid\alpha^p\in F\}$，**$F^{1/p}$ 是 Ω/F 的中间域．** K 是 F 的可分扩域必要且只要 K 与 $F^{1/p}$ 在 F 上线性无缘．

证 设 K 是 F 的一个可分扩域．我们证明，K 的在 F 上任意的有限生成子域与 $F^{1/p}$ 在 F 上线性无缘．

设 $F\subseteq E\subseteq K$，E/F 是有限生成的．则 E 是 F 上有限次可分扩域．于是由2.1.3，存在 $\alpha\in E$，使得 $E=F(\alpha)$．令 $f(X)\in F[X]$ 是 α 在 F 上的最小多项式，则 $1,\alpha,\cdots,\alpha^{n-1}$ $(n=\deg f)$ 作成 E 在 F 上一个基，于是根据 4.3.4，为了证明 E 与 $F^{1/p}$ 在 F 上线性无缘，只需证明 $1,\alpha,\cdots,\alpha^{n-1}$ 在 $F^{1/p}$ 上线性无关．

设 $h(X)\in F^{1/p}[X]$ 是 α 在 $F^{1/p}(\supseteq F)$ 上的最小多项式．那么在 $F^{1/p}[X]$ 内，$h(X)\mid f(X)$，另一方面 $h(X)^p\in F[X]$，所以在 $F[X]$ 内，$f(X)\mid h(X)^p$．因为 $h(X)$ 是 $F^{1/p}[X]$ 里的不可约多项式，而 $f(X)$ 是可分多项式，于是由 $F^{1/p}[X]$ 内因式分解的唯一性得出 $f(X)=h(X)$．这样，

$$[F(\alpha):F]=\deg f=\deg h=[F^{1/p}(\alpha):F^{1/p}].$$

所以 $1,\alpha,\cdots,\alpha^{n-1}$ 在 $F^{1/p}$ 上线性无关．

反过来，设 K 与 $F^{1/p}$ 在 F 上线性无缘．我们证明，K 中任意元素 α 都是 F 上的可分元素．

设 $\alpha\in K$．令 $f(X)$ 是 α 在 F 上的最小多项式，$\deg f=n$．则 $1,\alpha,\cdots,\alpha^{n-1}$ 在 F 上线性无关，而 K 与 $F^{1/p}$ 在 F 上线性无缘，所

以1, $\alpha, \cdots, \alpha^{n-1}$也在$F^{1/p}$上线性无关。如果$\alpha$不是$F$上的可分元素，那么存在$g(X)\in F[X]$，使得$f(X)=g(X^p)$。设

$$g(X)=\sum_{i=0}^{m} b_i X^i,\quad m=n/p.$$

则

$$h(X)=\sum_{i=0}^{m} b_i^{1/p} X^i\in F^{1/p}[X].$$

而

$$h(X)^p=g(X)^p=f(X).$$

于是$h(\alpha)^p=f(\alpha)=0$，从而$h(\alpha)=0$。这样一来，$1,\alpha,\cdots,\alpha^m$在$F^{1/p}$上线性相关。然而$m=n/p<n$。这就导致矛盾。 ▮

现在我们给出一般的可分扩张的定义。

设F是一个域，$\mathrm{char}F=p$，p是一个素数或0。K是F的一个扩域，Ω是K的一个代数闭包。如果$p=0$，我们约定$F^{1/p}=F$；如果$p>0$，令

$$F^{1/p}=\{\alpha\in\Omega\mid \alpha^p\in F\}.$$

域K叫做域F上一个**可分扩域**（域扩张K/F叫做**可分扩张**），如果K与$F^{1/p}$在F上线性无缘。

根据这个定义，特征为0的域F的任意扩域都是F上的可分扩域。由4.5.1，当K/F是代数扩张时，这个定义与在2.7所给的定义是一致的。

现在我们证明关于可分域扩张的几个等价的命题。

设F是一个域，$\mathrm{char}F=p$，p是一个素数或0。K是F的一个扩域，Ω是K的一个代数闭包。ν是一个非负整数。当$p>0$时，定义

$$K^{p^\nu}=\{\alpha^{p^\nu}\mid \alpha\in K\},$$
$$F^{1/p^\nu}=\{\alpha\in\Omega\mid \alpha^{p^\nu}\in F\}$$

K^{p^ν}是K的子域，F^{1/p^ν}是Ω/F的中间域。我们有

$$K\supseteq K^{p}\supseteq K^{p^2}\supseteq\cdots$$
$$F\subseteq F^{1/p}\subseteq F^{1/p^2}\subseteq\cdots\subseteq\Omega.$$

又约定

$$F^{1/p^\infty}=\bigcup_{\nu=0}^{\infty}F^{1/p^\nu}$$

那么F^{1/p^ν}也是Ω/F的一个中间域.

当$p=0$时，我们约定，$K^{p^\nu}=K$，$F^{1/p^\nu}=F^{1/p^\infty}=F$.

定理 4.5.2 设F是一个扩域，char $F=p$，p是一个素数或0。K是F的一个扩域，Ω是K的一个代数闭包. 下列条件是等价的:

(i) K/F是可分扩张;

(ii) K^p与F在F^p上线性无缘;

(iii) 对于任意非负整数ν，K^{p^ν}与F在F^{p^ν}上线性无缘;

(iv) 对于K的任意扩域M和F上任意一个纯不可分的代数扩域L，$F\subseteq L\subseteq M$，K与L在F上线性无缘.

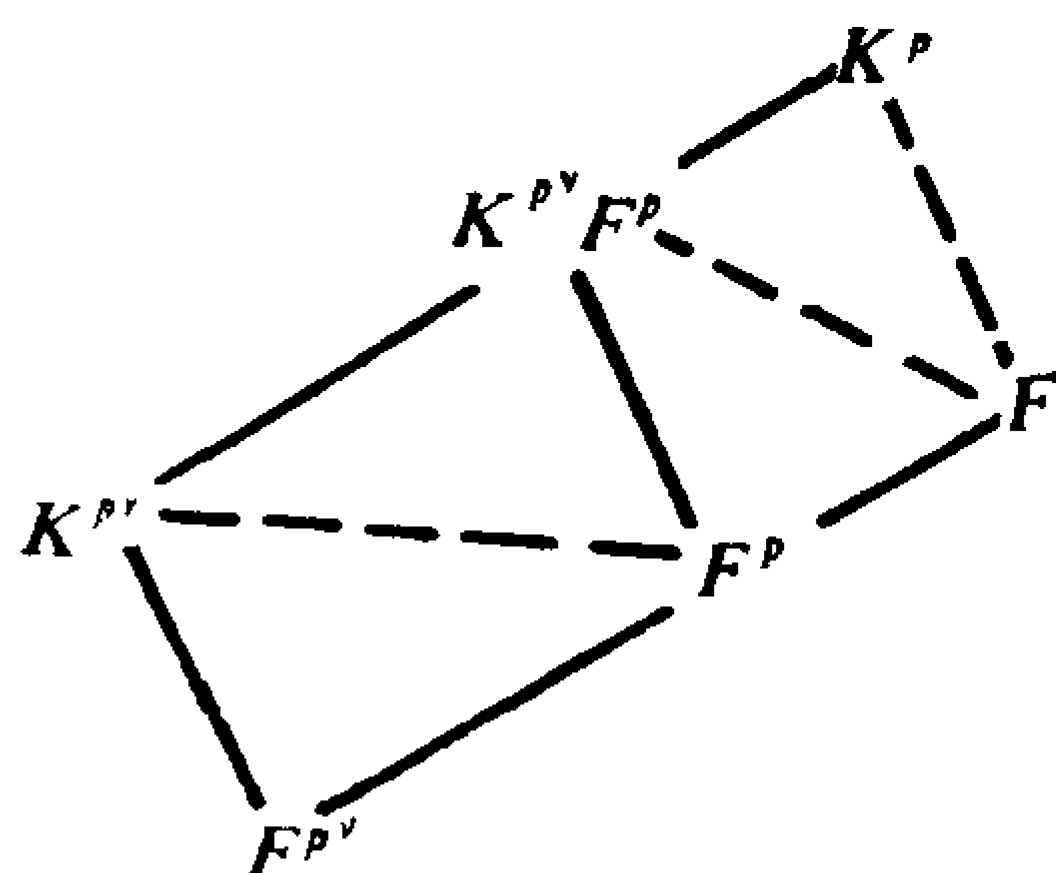
(v) K与F^{1/p^∞}在F上线性无缘;

(vi) 对于任意非负整数ν，K与F^{1/p^ν}在F上线性无缘.

证 当$p=0$时，$F=F^{p^\nu}=F^{1/p^\nu}=F^{1/p^\infty}, K^{p^\nu}=K, L=F$. 所以(i)—(vi)自然都是等价的. 设$p>0$.我们证明(i)—(vi)的等价性.

(i)$\Longrightarrow$(ii) $\omega:\Omega\ni\xi\longmapsto\xi^p\in\Omega$是$\Omega$的一个自同构，我们有$\omega(K)=K^p$, $\omega(F^{1/p})=F$, $\omega(F)=F^p$.因为K与$F^{1/p}$在F上线性无缘，所以$\omega(K)$与$\omega(F^{1/p})$在$\omega(F)$上线性无缘.

(ii)$\Longrightarrow$(iii) $\nu=0$时是明显的; $\nu=1$时就是(ii). 设$\nu\geqslant1$，并且假设$K^{p^{\nu-1}}$与F在$F^{p^{\nu-1}}$上线性无缘. 于是$K^{p^\nu}=\omega(K^{p^{\nu-1}})$与$F^p=\omega(F)$在$F^p=\omega(F^{p^{-1}})$上线性无缘. 然而$K^{p^\nu}\subseteq K^p$，$F^p\subseteq K^p$，所以$K^{p^\nu}F^p\subseteq K^p$. 因为$K^p$与$F$在$F^p$上线性无缘，所以$K^{p^\nu}F^p$与$F$也在$F^p$上线性无缘. 于是由4.3.5.



K^{p^ν}与F在F^{p^ν}上线性无缘。

(iii)$\Longrightarrow$(iv) 设M是K的任意一个扩域，L是M/F的一个中间域且L/F是纯不可分的代数扩张。我们证明，K与L在F上线性无缘。为此，只需证明，对于L的任意一个包含F的有限次子域L'，$F\subseteq L'\subseteq L$，$[L':F]<\infty$，K与L'在F上线性无缘。因此不妨设$[L:F]<\infty$。因为L/F是有限次纯不可分扩张，由2.8.4，存在一个非负整数e，使得$L^{p^e}\subseteq F$。然而由(iii)，K^{p^e}与F在F^{p^e}上线性无缘，所以K^{p^e}与L^{p^e}在F^{p^e}上线性无缘。考虑

$$\sigma: M^{p^e}\ni\xi^{p^e}\longmapsto\xi\in M.$$

这是M^{p^e}到M内的同态单射。显然$\sigma(K^{p^e})=K$，$\sigma(L^{p^e})=L$，$\sigma(F^{p^e})=F$。所以K与L在F上线性无缘。

(iv)$\Longrightarrow$(v) 设$\alpha\in F^{1/p^\infty}$。那么存在某一个整数$e\geqslant 0$，使得$\alpha\in F^{1/p^e}$，从而$\alpha^{p^e}\in F$。于是由2.8.2，F^{1/p^∞}是F的一个纯不可分代数扩域，且$F\subseteq F^{1/p^\infty}\subseteq\Omega$，由(iv)，$K$与$F^{1/p^\infty}$在$F$上线性无缘。

(v)$\Longrightarrow$(vi) 对于任意$\nu\geqslant 0$，$F^{1/p^\nu}\subseteq F^{1/p^\infty}$。

(vi)$\Longrightarrow$(i) 显然。 ▌

推论 4.5.3 设K是域F上的一个可分扩域，E是K/F的一个中间域。则E是F上的可分扩域。

证 令Ω是K的一个代数闭包。$F^{1/p}=\{\alpha\in\Omega\mid\alpha^p\in F\}$。因为$K/F$可分，所以$K$与$F^{1/p}$在$F$上线性无缘，因而$E$与$F^{1/p}$在$F$上线性无缘。 ▌

推论 4.5.4 设$F\subseteq E\subseteq K$是一串扩域。如果E/F和K/E都

是可分扩张，则K/F也是可分扩张。

证 令Ω是K的一个代数闭包。那么

$$F^{1/p}=\{\alpha\in\Omega\mid\alpha^p\in F\}\subseteq E^{1/p}=\{\alpha\in\Omega\mid\alpha^p\in E\}.$$

所以$F^{1/p}E=E(F^{1/p})\subseteq E^{1/p}$。由题设，$K$与$E^{1/p}$在$E$上线性无缘，所以$K$与$F^{1/p}E$在$E$上线性无缘。又$E$与$F^{1/p}$在$F$上线性无缘。于是由4.3.5，$K$与$F^{1/p}$在$F$上线性无缘。 ▌

注意 如果K/F是可分扩域，而E是K/F的一个中间域，一般来说，K/E不一定是可分的。参看定理4.5.5下面的例。

定理 4.5.5 一个域F的任意纯超越扩域K都是F上的可分扩域。

证 $\mathrm{char}F=0$时是显然的。设$\mathrm{char}F=p>0$。令B是K/F的一个超越基。$K=F(B)$，则K是整环$R=F[B]$的商域。根据4.3 3，我们只需证明，R的一个基在$F^{1/p}$上线性无关。

一切关于B中有限个元素的单项式

$$M_{(i)}(x)=x_1^{i_1}\cdots x_n^{i_n},\ x_j\in B, i_j\geqslant 0\ (1\leqslant j\leqslant n),$$

所组成的集是R在F上一个基。如果有

$$\sum\alpha_{(i)}M_{(i)}(x)=0,$$

$\sum$是有限和，$\alpha_{(i)}\in F^{1/p}$，那么

$$\sum\alpha_{(i)}^p M_{(i)}(x)^p=0,$$

$\alpha_{(i)}^p\in F$。因为B在F上代数无关，而$M_{(i)}(x)^p$是两两不同的单项式，所以$\alpha_{(i)}^p=0$，于是$\alpha_{(i)}=0$，$\forall(i)$。这就证明了$\{M_{(i)}(x)\}$在F上线性无关。 ▌

例 设F是一个域，$\mathrm{char}F=2$，t是F上一个超越元。令Ω是域$F(t)$的一个代数闭包，$u\in\Omega$是$F(t)$上多项式$X^3-(t^2+1)$的一个根：$u^3=t^2+1$。令$K=F(t,u)\subseteq\Omega$.那么K是$F(t)$上可分扩域；又由4.5.5，$F(t)$是F上可分扩域。所以K是F上可分扩域。

然而另一方面，我们有$t^2=u^3-1$，所以t是$F(u)$上多项式

$X^2-(u^3-1)$的根．而$K=F(u)(t)$是$F(u)$的纯不可分扩域．

最后再给出关于完备域的一个进一步的性质．回忆在2.9中的定义．一个域称为完备的，如果它的任何代数扩域都是可分的．现在我们证明，"代数"这个限制可以去掉．

定理 4.5.6 一个域是完备的必要且只要它的任意扩域都是可分的．

证 设F是一个域．$\mathrm{char}F=0$的情形是显然的．设$\mathrm{char}F=p>0$．

设F是完备的．则$F=F^p$．令K是F的任意一个扩域，则K^p与F在$F=F^p$上线性无缘，因而由4.5.2，K/F是可分扩张．

反之显然． ▮

习 题

1. 设K是域F的一个扩域．证明，K在F上可分必要且只要对于K中任意有限个元素$\alpha_1,\cdots,\alpha_n$来说，$F(\alpha_1,\cdots,\alpha_n)$在$F$上可分．

2. 设F是一个域，$\mathrm{char}F=p$，这里p或者是素数，或者等于零，M是F的一个扩域．对于M的元素α和整数$\nu\geqslant 0$，当$p>0$时，α^{p^ν}表示通常的α的p^ν次幂，当$p=0$时，约定$\alpha^{p^\nu}=\alpha$．令

$$M_i=\{\alpha\in M\mid \alpha^{p^\nu}\in F \text{对某一} \nu\geqslant 0\}.$$

证明．M_i是M/F的一个中间域，它是M中在F上纯不可分元素的全体．M_i称为F在F中的**纯不可分闭包**．

3. 设K是域F的一个扩域．证明，下列四个条件等价：

（i） K是F上的可分扩域；

（ii） 对于K的任意扩域M，令M_i是F在M中的纯不可分闭包，则M_i与K在F上线性无缘；

（iii） 设M是F的任意扩域，L是M/F的中间域，且L是

F 上一个纯不可分（代数）扩域，则K与L在F上线性无缘；

（iv） 设Ω是K的一个代数闭包，Ω_i是F在Ω内的纯不可分闭包，则Ω_i与K在F上线性无缘.

4. 设F是一个特征为$p>0$的域. 证明，域扩张K/F是可分的必要且只要对于K中任意一组在F上线性无关的元素$u_1,\cdots,u_n$来说，$u_1^p,\cdots,u_n^p$也在F上线性无关.

4.6 可分生成的扩域

设K是域F的一个扩域. K在F上一个超越基B说是**可分的**，如果K是$F(B)$上可分（代数）扩域. K叫做域F上的一个**可分生成的扩域**，如果存在K在F上一个可分超越基B，使得K是$F(B)$上一个可分（代数）扩域.

定理 4.6.1 设F是一个域.

（i） F上可分生成的扩域都是可分扩域.

（ii） F上有限生成的可分扩域都是可分生成的扩域.

证 （i） 设K是F上一个可分生成的扩域. 那么存在K/F的一个可分超越基B，使得K是$F(B)$上可分扩域. 又由4.5.5，$F(B)$是F上可分扩域. 所以K是F上可分扩域.

（ii） 设$K=F(\alpha_1,\cdots,\alpha_n)$是$F$上一个可分扩域. 我们证明，在$\{\alpha_1,\cdots,\alpha_n\}$中可以选出$K/F$的一个可分超越基.

如果char$F=0$，那么由4.1.4，在$\{\alpha_1,\cdots,\alpha_n\}$中可以选出$K/F$的一个超越基，这时$K/F$的任意一个超越基自然都是可分的.

现在设char$F=p>0$. 我们对n作归纳法. $n=0$时，$K=F$，$B=\varnothing$，论断(ii)显然成立. 假设对于F上任意一个由$n-1$个元素生成的可分扩域$E=F(\beta_1,\cdots,\beta_{n-1})$来说，可以在$\{\beta_1,\cdots,\beta_{n-1}\}$中选取一个可分超越基. 令$K=F(\alpha_1,\cdots,\alpha_n)$是$F$上一个可分扩域. 如果$\alpha_1,\cdots,\alpha_n$在$F$上代数无关，那么$\{\alpha_1,\cdots,$

$\alpha_n\}$就是K/F的一个可分超越基。设$\alpha_1,\cdots,\alpha_n$在F上代数相关，适当编号，可设$\alpha_1,\cdots,\alpha_r(0\leqslant r<n)$是$K/F$的一个超越基。那么$\alpha_1,\cdots,\alpha_{r+1}$在$F$上代数相关。于是存在非零多项式$f(X_1,\cdots,X_{r+1})\in F[X_1,\cdots,X_{r+1}]$，使得

$$f(\alpha_1,\cdots,\alpha_{r+1})=0.$$

不妨设$f\in F[X_1,\cdots,X_{r+1}]$是满足这一条件的非零多项式中次数最低的一个。则$f(X_1,\cdots,X_{r+1})$不可约。我们断言，不存在$g\in[X_1,\cdots,X_{r+1}]$，使得

$$f(X_1,\cdots,X_{r+1})=g(X_1^p,\cdots,X_{r+1}^p).$$

事实上，如果有

$$g=\sum a_{(i)}X_1^{i_1}\cdots X_{r+1}^{i_{r+1}}\in F[X_1,\cdots,X_{r+1}],$$

$a_{(i)}\in F$，使得

$$f(X_1,\cdots,X_{r+1})=\sum a_{(i)}X_1^{pi_1}\cdots X_{r+1}^{pi_{r+1}},$$

令

$$h(X_1,\cdots,X_{r+1})=\sum a_{(i)}^{1/p}X_1^{i_1}\cdots X_{r+1}^{i_{r+1}}\in$$
$$\in F^{1/p}[X_1,\cdots,X_{r+1}],$$

则$h(\alpha_1,\cdots,\alpha_{r+1})^p=f(\alpha_1,\cdots,\alpha_{r+1})=0$. $\deg h<\deg f$.
令$\{M_{(i)}(X)=X_1^{i_1}\cdots X_{r+1}^{i_{r+1}}\}$是出现在$h(X_1,\cdots,X_{r+1})$中一切单项式的集，令$M_{(i)}(\alpha)=\alpha_1^{i_1}\cdots\alpha_{r+1}^{i_{r+1}}$，则$\{M_i(\alpha)\}$在$F^{1/p}$上线性相关。然而根据题设，$K$与$F^{1/p}$在$F$上线性无缘，因此单项式集$\{M_{(i)}(\alpha)\}$也必须在$F$上线性相关。于是有线性关系

$$\sum b_{(i)}M_{(i)}(\alpha)=\sum b_{(i)}\alpha_1^{i_1}\cdots\alpha_{r+1}^{i_{r+1}}=0,$$

$b_{(i)}\in F$，且$b_{(i)}$不全为零。令

$$u(X_1,\cdots,X_{r+1})=\sum b_{(i)}X_1^{i_1}\cdots X_{r+1}^{i_{r+1}}.$$

则$u\in F[X_1,\cdots,X_{r+1}]$，$u\neq 0$且$u(\alpha_1,\cdots,\alpha_{r+1})=0$。然而$\deg u<\deg f$，这与$f$的取法矛盾。

这样，一定有某一个$X_i(1\leqslant i\leqslant r+1)$，$X_i$在$f$中出现，但不以$p$次幂出现。不妨设$i=1$。于是$f(X_1,\alpha_2,\cdots,\alpha_{r+1})$作为

$F(\alpha_2,\cdots,\alpha_{r+1})$上关于$X_1$的多项式，是可分的。然而$f(\alpha_1\alpha_2,\cdots,\alpha_{r+1})=0$，所以$\alpha_1$是$F(\alpha_2,\cdots,\alpha_{r+1})$上的可分元素，因而是$E=F(\alpha_2,\cdots,\alpha_n)$上的可分元素。

我们有$F\subseteq E\subseteq K$。因为K/F是可分的，所以由4.5.3，E/F是可分的，于是由归纳法的假设，在$\{\alpha_2,\cdots,\alpha_n\}$中可以选出$E/F$的一个可分超越基$B$。$E$是$F(B)$上可分代数扩域，而$K=E(\alpha_1)$是$E$上可分代数扩域，所以$K$是$F(B)$上可分代数扩域，而$B$是$K/F$的一个可分超越基。 ▮

由定理4.6.1的证明可以直接得出以下两个推论。

推论 4.6.2 设$K=F(\alpha_1,\cdots,\alpha_n)$是域$F$的一个有限生成的可分扩域，那么在$\{\alpha_1,\cdots,\alpha_n\}$中可以选出$K/F$的一个可分超越基。 ▮

推论 4.6.3 设F是一个完备域，K是F上一个有限生成的扩域。则K是F上可分生成的扩域。 ▮

下面的两个例子告诉我们，一个域F上的可分扩域不一定是可分生成的；即使是可分生成的，也不一定每一个超越基都是可分的。

例 1 设F是一个特征为$p>0$的域。$K=F(t)$，t是F上一个超越元。K自然是F上可分生成的扩域，$\{t\}$就是K/F的一个可分超越基。然而$\{t^p\}$也是K/F的一个超越基，但是$K/F(t^p)$是纯不可分扩张。

例 2 设F是一个特征为$p>0$的完备域。$E=F(t)$，t是F上一个超越元。令Ω是E的一个代数闭包。多项式$X^{p^\nu}-t\in E[X]$的根是$t^{p^{-\nu}}$，令$K=F(t,t^{p^{-1}},t^{p^{-2}},\cdots)=\bigcup_{\nu\geqslant 1}E(t^{p^{-\nu}})\subseteq\Omega$。因为$E$是完备域，所以由4.5.6，$K$是$F$上可分扩域。

然而K/F不是可分生成的。事实上，$\mathrm{tr.deg}_F K=1$。假设$\{u\}$是K/F的一个可分超越基。那么存在一个整数$e\geqslant 1$，使得

$$F(u)\subseteq F(t,t^{p^{-1}},\cdots,t^{p^{-e}}) = F(t^{p^{-e}})=E(t^{p^{-e}})=K'.$$

对于任意整数 $\nu\geqslant e+1$，令

$$K'_\nu=F(t,t^{p^{-1}},\cdots,t^{p^{-\nu}})=E(t^{p^{-\nu}}).$$

因为 $K/F(u)$ 是可分代数扩张，而 $F(u)\subseteq K'\subseteq K'\subsetneqq K$，所以 K'_ν/K' 是可分代数扩张，另一方面，多项式 $X^{p^\nu}-t\in E[X]$ 是不可约的（利用 Eisenstein 判别法很容易看出），所以 $[K'_\nu:E]=p^\nu$，从而 $[K'_\nu:K']=p^{\nu-e}>1$. 因此 K'_ν/K' 是纯不可分扩张. 这就导致矛盾.

定理 4.6.4 设 K 和 L 都是域 F 的扩域，并且被包含在某一个共同的扩域 M 内. K/F 是可分扩张，并且 K 与 L 在 F 上代数无关. 那么合成域 KL 是 L 上的可分扩域.

证 首先注意，$KL=L(K)$ 的每一个元素都可以表示成

$$f(\alpha_1,\cdots,\alpha_m)/g(\alpha_1,\cdots,\alpha_m),$$
$$f,g\in L[X_1,\cdots,X_m],g(\alpha_1,\cdots,\alpha_m)\neq 0,$$

的形式. 因此 KL 的任意一个在 L 上有限生成的子域都包含在一个合成域 $K'L$ 内. 这里 $K'\subseteq K$ 并且是 F 上有限生成的. 由 4.5.3，K'/F 是可分的. 这样，不失一般性，我们可以假设 K 是 F 上有限生成的.

设 K 是 F 上一个有限生成的可分扩域. 由 4.6.1，K 是 F 上可分生成扩域. 令 $\{t_1,\cdots,t_n\}$ 是 K 在 F 上一个可分超越基，令 $E=F(t_1,\cdots,t_n)$. 则 K/E 是可分代数扩张. 由题设，$t_1,\cdots,t_n$ 在 L 上代数无关，所以 $\{t_1,\cdots,t_n\}$ 也是 $KL=L(K)$ 在 L 上一个超越基. 在 KL 中，K 的每一个元素在 $E=F(t_1,\cdots,t_n)$ 上是可分代数元，因而也是 $EL=L(t_1,\cdots,t_n)$ 上的可分代数元. 由此 KL 是 $L(t_1,\cdots,t_n)$ 上可分代数扩域，$\{t_1,\cdots,t_n\}$ 是 K/L 的一个可分超越基，这样，KL 是 L 上可分生成的扩域. 因而是可分扩域. ▌

习 题

1. 设K和L都是域扩张M/F的中间域，并且K和L都是F上可分扩域。如果K与L在F上代数无关，则KL是F上可分扩域。

2. 设K和L都是域扩张M/F的中间域，且K与L在F上线性无缘。证明，K/F可分必要且只要KL/L可分。

3. 设F是一个特征为$p>0$的完备域，K是F上一个非完备扩域，又$\mathrm{tr.deg}_F K=1$。证明，K是F上可分生成的。

4. 设F_0是一个特征为$p>0$的域，x,y,z是F_0上代数无关的元素。令$K=F_0(x,y,z,u)$，$u^p=xy^p+y$。证明：

(i) $F=F_0(x,y)$在K中是代数闭的；

(ii) K/F不是可分生成的。

4.7 导 子

在这一章的最后一节，我们介绍一下导子的概念。导子是通常导数概念的自然推广，它在域论和代数的其它一些分支中都占有一定的重要地位。

设R是一个有单位元1的交换环，A是R的一个子环，并且A含有R的单位元。在这一节里，说到R和A，都作这样理解。

A到R的一个映射$D: A\to R$叫做A到R的一个**导子**，如果下列两个条件被满足：

(1) $$D(a+b)=D(a)+D(b);$$

(2) $$D(ab)=aD(b)+bD(a),$$

这里a,b是A的任意元素。

环R到R的导子叫做R**的导子**。

例1 设$R=F[X_1,\cdots,X_n]$是某一个域F上n元多项式环。对于每一个X_i和$f\in R$，令$\partial f/\partial X_i$表示f关于X_i的偏导数，也

就是将 f 看成整环 $F[X_1,\cdots,X_{i-1},X_{i+1},\cdots,X_n]$ 上关于 X_i 的一元多项式对 X_i 的导数．那么

$$\partial/\partial X_i: R\ni f\longmapsto \partial f/\partial X_i\in R$$

是 R 的导子．

定理 4.7.1 设 $D: A\to R$ 是 A 到 R 的一个导子．则

(i) $D(1)=0$，$D(0)=0$，$D(-a)=-D(a)$，$\forall a\in A$；

(ii) $S=\{a\in A\mid D(a)=0\}$ 作成 A 的一个子环；

(iii) $D(a^n)=na^{n-1}D(a)$，$a\in A$，n 是任意正整数；

(iv) 对于 $a,b\in A$，且 b 是一个可逆元素，

$$D(a/b)=(bD(a)-aD(b))/b^2.$$

证 (i) 由(2)，$D(1)=D(1^2)=D(1)+D(1)\Longrightarrow D(1)=0$．由(1)，$D(0)=D(0+0)=D(0)+D(0)\Longrightarrow D(0)=0$．于是，

$$D(a)+D(-a)=D(a+(-a))=D(0)=0.$$
$$\Longrightarrow D(-a)=-D(a).$$

(ii) 由(i)及(2)，对于 $a,b\in S$，我们有 $a-b\in S$，$ab\in S$．所以 S 是 A 的子环．

(iii) 由(2)，对 n 作归纳法．

(iv) 设 b 是 A 的一个可逆元素．那么

$$0=D(1)=D(bb^{-1})=bD(b^{-1})+b^{-1}D(b).$$

所以，$D(b^{-1})=-b^{-2}D(b)$．于是

$$D(a/b)=D(ab^{-1})=aD(b^{-1})+b^{-1}D(a)$$
$$=-ab^{-2}D(b)+b^{-1}D(a)=b^{-2}(bD(a)-aD(b)).\qquad\blacksquare$$

设 B 是 R 的一个子环，且 $A\subseteq B\subseteq R$．令 D 是 A 到 R 的一个导子．如果 $\bar{D}: R\to R$ 是 B 到 R 的一个导子，且 $\bar{D}|_A=D$，那么就说 $\bar{D}$ 是 D 在 B 上一个**开拓**．

把 A 的每一个元素都映成零元的零映射显然是 A 的一个导子，称为**平凡导子**．设 $D: R\to R$ 是 R 的一个导子，A 是 R 的一个子环．如果 $D|_A$ 是 A 的平凡导子，那么就说 **D 在 A 上是平凡的**，

或者说D是A上的导子．这时D是R的一个A-线性映射，因为对于$a\in A$，$\alpha\in R$，都有$D(a\alpha)=aD(\alpha)$．

设F是一个域，F_0是F的素域．那么或者$F_0\cong Q$，或者$F_0\cong F_p$．由4.7.1容易看出，F的每一个导子都是在F_0上平凡的．

例2　设D是环R的一个导子．令$P=R[X_1,\cdots,X_n]$是R上n元多项式环．则D可以看成R到P的一个导子．对于

$$f=\sum_{(i)=(i_1,\cdots,i_n)}a_{(i)}X_1^{i_1}\cdots X_n^{i_n}\in P.$$

定义

$$f^D=\sum_{(i)}D(a_{(i)})X_1^{i_1}\cdots X_n^{i_n}.$$

那么映射$P\ni f\longmapsto f^D\in P$是$P$的一个导子，它是$D$在$P$上的一个开拓．

现在设R是一个整环，F是R的商域．R的导子可以看成R到F的导子．我们看R的导子在F上的开拓．

定理 4.7.2　设R是一个整环，F是R的商域．R的每一个导子D都可以唯一地开拓为F的一个导子$\tilde{D}$：对于$a,b\in R,b\neq 0$,

$$\tilde{D}(a/b)=(bD(a)-aD(b))/b^2.$$

证　如果$a/b=a'/b'$，$a,a',b,b'\in R$，则$ab'=a'b$．于是

$$aD(b')+b'D(a)=a'D(b)+bD(a'),$$

从而

$$b'(D(a)-(a'/b')D(b))=b(D(a')-(a/b)D(b')).$$

因为$a/b=a'/b'$，所以

$$(D(a)-(a/b)D(b))/b=(D(a')-(a'/b')D(b'))/b',$$

即

$$(bD(a)-aD(b)/b^2=(b'D(a')-a'D(b'))/b'^2.$$

这样，定义

$$\tilde{D}(a/b)=(bD(a)-aD(b))/b^2$$

不依赖于a/b的表示法，所以$\tilde{D}:F\to F$是一个映射．直接验证可知条件(1)，(2)都被满足，所以$\tilde{D}$是F的一个导子，并且是D

在 F 上的开拓.

设D'也是D在F上一个开拓. 那么由4.7.1 (iv), 必须有

$$
\begin{aligned}
D'(a/b) &= (bD'(a) - aD'(b))/b^2 \\
&= (bD(a) - aD(b))/b^2 = \tilde{D}(a/b).
\end{aligned}
$$ ▮

现在设 F 是一个域. $K = F(\alpha_1, \cdots, \alpha_n)$是 $\alpha_1, \cdots, \alpha_n$ 在 F 上所生成的扩域. 我们考虑 F 的导子在 K 上的开拓.

令 $F[X_1, \cdots, X_n]$是F上 n 元多项式环. 我们以下把它简记作 $F[X]$. 对于 $f \in F[X]$, 我们将 $f(\alpha_1, \cdots, \alpha_n)$简记作 $f(\alpha)$ 并且记

$$
\left(\frac{\partial f}{\partial X_i}\right)_\alpha = \frac{\partial f}{\partial X_i}(\alpha_1, \cdots, \alpha_n).
$$

设 D 是 F 的一个导子. 我们问, 是否存在 K 的导子 $\tilde{D}$, 使得 $\tilde{D}$ 是 D 的开拓? 如果 $\tilde{D}: K \to K$ 是这样一个开拓, 那么对于任意 $f \in F[X]$且 $f(\alpha) = 0$, 以下等式成立:

$$
(3) \qquad f^D(\alpha) + \sum_{i=1}^{n} \left(\frac{\partial f}{\partial X_i}\right)_\alpha \tilde{D}(\alpha_i) = \tilde{D}(f(\alpha)) = 0,
$$

这里 f^D 的意义如例2. 令

$$
I = \{f \in F[X] \mid f(\alpha) = 0\}.
$$

则 I 是$F[X]$的一个理想, 叫做$(\alpha) = (\alpha_1, \cdots, \alpha_n)$在 $F[X]$ 内所确定的理想. 令 $\{f_\lambda\}_{\lambda \in \Lambda}$ 是 I 的一组生成元[1]. 那么 I 的每一个元素 f 都可以写成 $f = \sum_\lambda g_\lambda f_\lambda$ (有限和), $g_\lambda \in F[X]$. 因此根据导子的定义容易证明, 如果每一个生成元 $f_\lambda (\lambda \in \Lambda)$ 都满足关系式(3), 则 I 中每一个多项式 f 也满足关系式(3).

下面的定理告诉我们, 关系式(3)也是导子 $\tilde{D}$存在的充分条件.

1) 在下一章里将会看到, $F[X]$的任意理想都可以由有限个元素生成(参看5.2.5).

定理 4.7.3 设$K=F(\alpha_1,\cdots,\alpha_n)$是$\alpha_1,\cdots,\alpha_n$在$F$上所生成的扩域，$D$是$F$的一个导子。令

$$I=\{f\in F[X]\mid f(\alpha)=0\}$$

是$(\alpha)=(\alpha_1,\cdots,\alpha_n)$在$F[X]$内所确定的理想，$\{f_\lambda\}_{\lambda\in\Lambda}$是$I$的一组生成元。如果$u_1,\cdots,u_n\in K$，满足以下的一组关系：

$$f_\lambda^D(\alpha)+\sum_{i=1}^{n}\left(\frac{\partial f_\lambda}{\partial X_i}\right)_\alpha u_i=0,\quad \forall\lambda\in\Lambda,$$

那么存在K的导子$\tilde{D}$，使得$\tilde{D}|_F=D$，并且$\tilde{D}(\alpha_i)=u_i, 1\leqslant i\leqslant n$。

证 设$f\in I$，则$f=\sum_{\lambda\in\Lambda}g_\lambda f_\lambda$（有限和）。因为$f_\lambda(\alpha)=0$，所以

$$f^D(\alpha)=\sum_{\lambda\in\Lambda}g_\lambda(\alpha)f_\lambda^D(\alpha),$$

$$\left(\frac{\partial f}{\partial X_i}\right)_\alpha=\sum_{\lambda\in\Lambda}g_\lambda(\alpha)\left(\frac{\partial f_\lambda}{\partial X_i}\right)_\alpha,\quad 1\leqslant i\leqslant n.$$

于是由题设的条件，我们有

$$f^D(\alpha)+\sum_{i=1}^{n}\left(\frac{\partial f}{\partial X_i}\right)_\alpha u_i=0.$$

令$R=F[\alpha_1,\cdots,\alpha_n]=\{f(\alpha)\mid f(X)\in F[X]\}$。则$R$是一个整环，并且$K$是$R$的商域。设$f(X),g(X)\in F[X]$。如果$f(\alpha)=g(\alpha)$，则$f-g\in I$。于是

$$f^D(\alpha)+\sum_{i=1}^{n}\left(\frac{\partial f}{\partial X_i}\right)_\alpha u_i=g^D(\alpha)+\sum_{i=1}^{n}\left(\frac{\partial f}{\partial X_i}\right)_\alpha u_i.$$

对于任意$v\in R$，则有$f(X)\in F[X]$，使得$v=f(\alpha)$。我们定义

$$D'(v)=f^D(\alpha)+\sum_{i=1}^{n}\left(\frac{\partial f}{\partial X_i}\right)_\alpha u_i.$$

则$D'(v)$不依赖于$f(X)$的选取。因而$v\longmapsto D'(v)$是R到K的一个映射。易证D'是一个导子，且$D'(\alpha_i)=u_i, 1\leqslant i\leqslant n$。由4.7.2，

D'可以唯一地开拓为K的导子$\tilde{D}$。 ▮

设$f_1,\cdots,f_m\in F[X_1,\cdots,X_n]$。$m\times n$矩阵

$$J(f_1,\cdots,f_m)=\begin{pmatrix}\dfrac{\partial f_1}{\partial X_1}\cdots\dfrac{\partial f_1}{\partial X_n}\\ \cdots\cdots\cdots\cdots\cdots\cdots\\ \dfrac{\partial f_m}{\partial X_1}\cdots\dfrac{\partial f_m}{\partial X_n}\end{pmatrix}$$

叫做$f_1,\cdots,f_m$的Jacobi矩阵。记

$$J(f_1,\cdots,f_m)_a=\begin{pmatrix}\left(\dfrac{\partial f_1}{\partial X_1}\right)_a\cdots\left(\dfrac{\partial f_1}{\partial X_n}\right)_a\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ \left(\dfrac{\partial f_m}{\partial X_1}\right)_a\cdots\left(\dfrac{\partial f_m}{\partial X_n}\right)_a\end{pmatrix}.$$

由4.7.3，我们立即得到以下

推论 4.7.4 记号同4.7.3。如果I由n个多项式$f_1,\cdots,f_m\in F[X]$生成，那么D在K上一切开拓与线性方程组

$$J(f_1,\cdots,f_m)_a\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}=-\begin{pmatrix}f_1^D(a)\\ \vdots\\ f_m^D(a)\end{pmatrix}$$

在K内的一切解之间存在着1-1对应。 ▮

现在考虑$K=F(\alpha)$是域F的单扩域的情形。我们有

定理 4.7.5 设$K=F(\alpha)$是域F的一个单扩域，D是F的一个导子。

(i) 如果α是F上的超越元，那么对于任意$\gamma\in K$，存在D在K上的开拓$\tilde{D}$，使得$\tilde{D}(\alpha)=\gamma$。

(ii) 如果α是F上可分代数元，那么D可以唯一地开拓为K的导子$\tilde{D}$。

(iii) 设$\mathrm{char}F=p>0$，α是F上不可分元素。令$f(X)$

是 α 在 F 上的最小多项式。那么 D 可以开拓为 K 的导子的充分且必要条件是 $f^D(\alpha)=0$。如果这个条件成立，那么对于任意 $\gamma\in K$，存在 D 在 K 上的开拓 $\tilde{D}$，使得 $\tilde{D}(\alpha)=\gamma$。

证 令 $I=\{f\in F[X]\mid f(\alpha)=0\}$ 是 α 在一元多项式环 $F[X]$ 内所确定的理想。

(i) 如果 α 是 F 上超越元，则 $I=(0)$。这时定理4.7.3的条件自然被满足。

(ii) 令 $f(X)$ 是 α 在 F 上的最小多项式。则 $I=(f)$。这时 $\partial f/\partial X=f'(X)$。因为 $f(X)$ 是可分的，所以 $f'(\alpha)\neq 0$。定理4.7.3的条件为 $f^D(\alpha)+f'(\alpha)u=0$。从而 $u=-f^D(\alpha)/f'(\alpha)$ 是唯一确定的。所以 D 可以唯一地开拓为 K 的导子 $\tilde{D}$，$\tilde{D}(\alpha)=u$。

(iii) 因为 α 是 F 上不可分元素，所以 $f'(X)=0$。

如果 D 可以开拓为 $\tilde{D}: K\to K$，则

$$f^D(\alpha)+f'(\alpha)\tilde{D}(\alpha)=0.$$

所以 $f^D(\alpha)=0$。

反之，设 $f^D(\alpha)=0$。那么对于任意，$\gamma\in K$，都有 $f^D(\alpha)+f'(\alpha)\gamma=0$，由4.7.3，存在 K 的导子 $\tilde{D}$, $\tilde{D}|_F=D$ 且 $\tilde{D}(\alpha)=\gamma$。 ▮

推论 4.7.6 设 $K=F(\alpha)$ 是域 F 的一个单扩域，$\mathrm{char}F=p>0$，且 $\alpha^p\in F$。令 D 是 F 的一个导子。D 可以开拓为 K 的导子必要且只要 $D(\alpha^p)=0$。

如果这个条件被满足，则对于任意 $\gamma\in K$，存在 D 在 K 上的开拓 $\tilde{D}$，使得 $\tilde{D}(\alpha)=\gamma$。

证 可设 $\alpha\notin F$。则 α 在 F 上的最小多项式是 $f(X)=X^p-a$，$a=\alpha^p\in F$，于是

$$f^D(X)=D(1)X^p-D(a)=-D(\alpha^p).$$

由定理4.7.4 (iii)，就得到这个推论。 ▮

推论 4.7.7 设$K=F(\alpha)$是域F的一个单扩域，$\gamma\in K$。

(i) 如果K/F是超越扩张或者是不可分的代数扩域，那么存在K在F上的导子D，使得$D(\alpha)=\gamma$。

(ii) 如果K/F是可分的代数扩张，那么K的任意在F上的导子都是K的平凡导子。 ▌

定理 4.7.8 设K是域F的一个扩域，D是F的一个导子。

(i) 如果$\mathrm{char}F=0$，那么D一定可以开拓为K的一个导子。这时，对于K的一个在F上的超越元z和任意$\gamma\in K$，总存在D在K上的一个开拓$\tilde{D}$，使得$\tilde{D}(z)=\gamma$。

(ii) 如果$\mathrm{char}F=p>0$且$F\supseteq K^p$。D可以开拓为K的导子必要且只要$D(K^p)=0$。这时，对给定$\beta\in K$，$\beta\notin F$和任意$\gamma\in K$，总存在D上的开拓$\tilde{D}$，使得$\tilde{D}(\beta)=\gamma$。

证 考虑这样的对(K',D')，其中K'是K/F的一个中间域，$D':K'\to K$是K'到K的导子且$D'|_F=D$。令M是一切这样的对(K',D')所成的集。显然$(F,D)\in M$，所以$M\neq\varnothing$。对于(K_1,D_1)，$(K_2,D_2)\in M$，规定

$$(K_1,D_1)<(K_2,D_2)\Longleftrightarrow K_1\subseteq K_2,\ \text{且}D_2|_{K_1}=D_1.$$

则M对于"$<$"作成一个偏序集。令$\{(K_\lambda,D_\lambda)\mid\lambda\in\Lambda\}$是$M$中一个链。令$K'=\bigcup_{\lambda\in\Lambda}K_\lambda$，则$F\subseteq K'\subseteq K$。设$\alpha'\in K'$，那么一定有某一$\lambda\in\Lambda$，使$\alpha'\in K_\lambda$。定义$D'(\alpha')=D_\lambda(\alpha')$。容易看出，$D'(\alpha)$不依赖于$\alpha'$所在的域$K_\lambda$的选取，并且$D'$是$K'$到$K$的一个导子，且$D'|_F=D$，所以$(K',D')\in M$，并且是$\{(K_\lambda,D_\lambda)\mid\lambda\in\Lambda\}$的一个上界。于是由Zorn引理，$M$有一个极大元素$(L,\tilde{D})$。我们证明，$L=K$。

(i) 设$\mathrm{char}F=0$，如果$L\subsetneqq K$，那么存在$\alpha\in K$，但$\alpha\notin L$，于是$L\subsetneqq L(\alpha)\subseteq K$。因为$\mathrm{char}F=0$，所以不论$\alpha$是$F$上的代数元（因而是可分代数元）还是超越元，由定理4.7.5，$\tilde{D}$

都可以开拓为$L(\alpha)$的导子D^*.从而$(L(\alpha),D^*)\in M$.这与$(L,\tilde{D})$的极大性矛盾．这样，必须$L=K$，$\tilde{D}:K\to K$是D在K上的开拓．

设 $z\in K$是F上一个超越元，那么由4.7.5，对于任意$\gamma\in K$,存在D在$F(z)$上的开拓$\bar{D}$，使得$\bar{D}(\alpha)=\gamma$.于是由上面的证明，对于域$F(z)$和$F(z)$的导子$\bar{D}$，存在$\bar{D}$在K上的开拓$\tilde{D}$，$\tilde{D}|_{F(z)}=\bar{D}$，所以$\tilde{D}|_F=D$，且$\tilde{D}(z)=\gamma$．

(ii) 设$\mathrm{char}F=p>0$．$K^p=\{a=\alpha^p|\alpha\in K\}\subseteq F$．如果$D$可以开拓为$K$的导子$\tilde{D}$，那么对于$a=\alpha^p\in K^p\subseteq F$,

$$D(a)=\tilde{D}(a)=\tilde{D}(\alpha^p)=p\alpha^{p-1}\tilde{D}(\alpha)=0.$$

所以$D(K^p)=0$．

反之，设$(L,\tilde{D})$是上述的M中的极大元．如果$L\subsetneqq K$，则存在$\alpha\in K,\alpha\notin L$,于是$L\subsetneqq L(\alpha)\subseteq K$.$\alpha^p\in K^p\subseteq F\subseteq L$．由题设，$\tilde{D}(\alpha^p)=0$．于是由4.7.6，$\tilde{D}$可以开拓为$L(\alpha)$的一个导子．这与$(L,\tilde{D})$的极大性矛盾．于是$L=K$，$\tilde{D}:K\to K$是$D$在$K$上的开拓．

(ii)的后一论断与(i)的后一论断的证明完全类似． ▮

推论 4.7.9 设K是域F的一个扩域，$\alpha\in K$．

(i) 在$\mathrm{char}F=0$的情形．对于K的任何一个在F上的导子D都有$D(\alpha)=0$，必要且只要α是F上的代数元．

(ii) 在$\mathrm{char}F=p>0$的情形.对于K的任何一个在F上的导子D都有$D(\alpha)=0$，必要且只要$\alpha\in K^pF$．

证 (i) 如果α是F上的超越元，由4.7.8(i)，总存在K的在F上的导子D，使得$D(\alpha)\neq 0$．

反之，设α是F上的代数元．则$F(\alpha)$是F的可分代数扩域．令D是K的一个导子且$D|_F=0$．令$D'=D|_{F(\alpha)}$，则D'是$F(\alpha)$的一个导子，$D'|_F=0$．D'是F的平凡导子D_0在$F(\alpha)$上的开拓．由4.7.5(ii)，D_0在$F(\alpha)$上只有唯一的开拓，而$F(\alpha)$

的平凡导子显然是D_0的一个开拓．所以$D'=0$，从而$D(\alpha)=0$．

(ii) 我们有 $K^p\subseteq K^pF\subseteq K$．如果 $\alpha\notin K^pF$，那么由 4.7.8 (ii)，存在K在K^pF上的导子D，使得 $D(\alpha)\neq 0$．D自然也是在F上平凡的．

反之，因为K的任意在F上的导子D都是F-线性变换．由导子的性质立即得出，对于任意 $\alpha\in K^pF$，都有$D(\alpha)=0$． ▌

推论 4.7.10 设F是一个域．$\alpha\in F$．

(i) 在$\mathrm{char}F=0$的情形．对于F的任意导子D都有$D(\alpha)=0$必要且只要α在F的素域F_0上是代数的．

(ii) 在$\mathrm{char}F=p>0$的情形．对于F的任意导子D都有$D(\alpha)=0$必要且只要$\alpha\in F^p$．

证 令F_0是F素域．则$F_0\cong \mathbf{Q}$，若$\mathrm{char}F=0$；$F_0\cong \mathbf{F}_p$，若$\mathrm{char}F=p>0$．F的每一个导子在F_0上都是平凡的．

(i) 由4.7.9 (i)直接得出．

(ii) $F_0=F_0^p\subseteq F^p$．所以$F^pF_0=F^p$．于是由 4.7.9 (ii)，就得出这里的论断(ii)． ▌

定理 4.7.11 设K是域F的一个扩域．

(i) 如果K/F是可分代数扩张，那么K的每一个在F上的导子也是K的平凡导子．

(ii) 设$K=F(\alpha_1,\cdots,\alpha_n)$是$F$上有限生成的扩域．如果$K$的每一个在$F$上的导子都是$K$的平凡导子，那么$K$是$F$的（有限次）可分代数扩域．

证 (i) 设D是K的一个在F上的导子．如果$D\neq 0$，那么一定有$\alpha\in K$，使得$D(\alpha)\neq 0$．于是$D|_{F(\alpha)}$是$F(\alpha)$的一个在F上的导子，但$D|_{F(\alpha)}\neq 0$．然而$F(\alpha)$是F的可分扩域．于是由4.7.7 (ii)，必须$D|_{F(\alpha)}=0$．这就导致矛盾．

(ii) 如果K不是F上可分代数扩域．令$F_0=F$，$F_i=F_{i-1}(\alpha_i)$，$1\leqslant i\leqslant n$，$F_n=K$，那么存在一个m，$1\leqslant m\leqslant n$，使得

K是F_m上的可分代数扩域但不是F_{m-1}上的可分代数扩域．于是F_m/F_{m-1}或者是超越扩张，或者是不可分的代数扩张．于是由4.7.7，存在F_m的导子$D\neq 0$，但$D|_{F_{m-1}}=0$．而$K=F_m(\alpha_{m+1},\cdots,\alpha_n)$是$F_m$上可分代数扩域．由4.7.5(ii)，$D$可以逐步开拓为$K$的一个导子$\tilde{D}$，$\tilde{D}\neq 0$但$\tilde{D}$在$F$上是平凡的．∎

定理 4.7.12 设K是域F的一个扩域．K是F上的可分扩域必要且只要F的每一个导子都可以开拓为K的一个导子．

证 当char$F=0$时，K/F是可分的．由4.7.8，F的每一个导子都可以开拓到K上．这时定理显然成立．

以下设char$F=p>0$．

设K是F的可分扩域．由4.5.2(ii)，F与K^p在F^p上线性无缘．令$\{u_i\}_{i\in I}$是F在F^p上一个基．则$\{u_i\}_{i\in I}$在K^p上线性无关．令$F[K^p]$是K^p在F上所生成的子整环，$F[K^p]\subseteq K$．那么

$$F[K^p]=\{\sum a_i\alpha_i^p\ (\text{有限和})\ |\ a_i\in F,\alpha_i\in K\}$$
$$=\{\sum u_i\alpha_i^p\ (\text{有限和})\ |\ \alpha_i\in K\}.$$

而且$\{u_i\}_{i\in I}$作成K^p上向量空间$F[K^p]$的一个基．设D是F的一个导子．则$D(F^p)=0$．因此D是F^p上向量空间F的一个线性变换．所以D可以开拓为K^p上向量空间$F[K^p]$的一个线性变换

$$D':F[K^p]\ni\sum u_i\alpha_i^p\longmapsto\sum D(u_i)\alpha_i^p\in F[K^p].$$

易证D'是$F[K^p]$的导子，且$D'(K^p)=0$，于是D'可以唯一地开拓为$F[K^p]$的商域$F(K^p)$的一个导子D''．因为$K\supseteq F(K^p)\supseteq K^p$，且$D''(K^p)=0$．于是由4.7.8，$D''$可以开拓到$K$上．

反过来，设F的任意导子D都可以开拓到K上．我们证明，K与$F^{1/p}$在F上线性无缘．

如果存在$u_1,\cdots,u_n\in K$，$u_1,\cdots,u_n$在F上线性无关，但是在$F^{1/p}$上线性相关，那么有$a_i\in F$，a_i不全为零$(1\leqslant i\leqslant n)$，使得$\sum_{i=1}^{n}a_i^{1/p}u_i=0$．于是

(4) $$\sum_{i=1}^{n} a_i u_i^p = 0 .$$

可设 n 是K中具有上述性质的元素的最小个数，则 $n\geqslant 2$，并且 $a_i\neq 0$ $(1\leqslant i\leqslant n)$。因此可设$a_n=1$，

令 $\bar{D}$是F的一个导子D在K上的开拓．对(4)式施行 $\bar{D}$．因为 $\bar{D}(u_i^p)=0$ $(1\leqslant i\leqslant n)$，$D(1)=0$，于是得到

$$\sum_{i=1}^{n-1} \bar{D}(a_i)u_i^p = 0 .$$

由 n 的最小性得 $\bar{D}(a_i)=0$，$1\leqslant i\leqslant n-1$。因为$D$可以是$F$的任意导子，由4.7.10(ii)，我们有$a_i=b_i^p\in F^p, 1\leqslant i\leqslant n, b_n=1$。于是(4)式化为$\sum_{i=1}^{n} b_i^p u_i^p=0 \Longrightarrow \left(\sum_{i=1}^{n} b_i u_i\right)^p=0$．从而

$$\sum_{i=1}^{n} b_i u_i = 0 ,\ b_i\in F, b_n=1 .$$

这与$u_1,\cdots,u_n$在F上线性无关的假设矛盾． ∎

设K是域F的一个扩域．令 $\mathrm{Der}(K/F)$ 表示一切K的在F上的导子所成的集．设$D, D'\in \mathrm{Der}(K/F)$，$a, b\in K$，我们定义

$$(D+D')(b)=D(b)+D'(b);$$
$$(aD)(b)=aD(b),$$

那么$\mathrm{Der}(K/F)$作成域K上一个向量空间．

定理 4.7.13 设 $K=F(X_1,\cdots,X_n)$是域F上n个不定元 $X_1,\cdots,X_n$的有理分式域．那么导子$\partial/\partial X_1,\cdots,\partial/\partial X_n$ 作成K F上向量空间$\mathrm{Der}(K/F)$的一个基．

证 设D是K在F上任意一个导子．$D(X_i)=u_i(1\leqslant i\leqslant n)$．令$D'=D-\sum_{i=1}^{n} u_i\partial/\partial X_i$．那么 $D'(X_i)=0$，$1\leqslant i\leqslant n$．所以 $D'=0$，从而$D=\sum_{i=1}^{n} u_i\partial/\partial X_i$．

如果$\sum_{i=1}^{n} v_i\partial/\partial X_i=0, v_i\in K$．因为 $\partial X_j/\partial X_i=\delta_{ij}$，这里

$\delta_{ij}=1$，若$i=j$，$\delta_{ij}=0$，若$i\neq j$. 于是$v_j=\sum_{i=1}^{n}v_i(\partial X_j/\partial X_i)=0$，$1\leqslant j\leqslant n$，所以$\partial/\partial X_1,\cdots,\partial/\partial X_n$在$K$上线性无关，因而作成$\mathrm{Der}(K/F)$的一个基。 ▌

设F是一个特征为$p>0$的域，K是F的一个扩域。令$L=K^pF$。K的一个子集S说是在F上**p-无关的**，如果对于S的任意有限个互不相同的元素$s_1,\cdots,s_n$来说，都有$[L(s_1,\cdots,s_n):L]=p^n$。

K的一个在F上p-无关的子集S说是**极大的**，如果不存在K的在F上p-无关的子集T，使得$T\supsetneqq S$。K在F上一个极大的p-无关子集叫做K在F上的一个**p-基**。

显然，如果S^*是K在F上一个p-基，那么$K=L(S^*)=K^pF(S^*)$。

定理 4.7.14 设K是域F的一个扩域，$\mathrm{char}F=p>0$.

(i) 任意给定K在F上一个p-无关的子集S，总存在K在F上一个p-基S^*，使得$S^*\supseteq S$。特别，K在F上的p-基一定存在。

(ii) 令S^*是K在F上一个p-基，Φ是一切S^*到K内的映射所成的集。那么存在$\mathrm{Der}(K/F)$到Φ的一个双射$\mathrm{Der}(K/F)\ni D\longmapsto\varphi_D\in\Phi$，使得$\varphi_D(s)=D(s)$，$\forall s\in S^*$。

证 (i) 利用Zorn引理很容易证明。

(ii) 设$D\in\mathrm{Der}(K/F)$. 则$D(K^pF)=0$，所以$\mathrm{Der}(K/F)=\mathrm{Der}(K/K^pF)$。因此，用$K^pF$代替$F$，并不影响定理的证明。这样，不失一般性，可以假设$K^p\subseteq F$。

对于$D\in\mathrm{Der}(K/F)$。令$\varphi_D: S^*\to S^*$，$\varphi_D(s)=D(s)$，$\forall s\in S^*$。则$\varphi_D\in\Phi$。所以$D\longmapsto\varphi_D$是$\mathrm{Der}(K/F)$到Φ的一个映射。我们证明，这个映射是双射。

设$\varphi\in\Phi$。令s是S^*的任意一个元素。令$S_s^*=S^*\setminus\{s\}$。则

$s \notin F(S_s^*)$，而$S^p \in F \subseteq F(S_s^*)$．由4.7.8，存在$K=F(S^*)$在$F(S_s^*)$上的导子$D_s: K \to K$，使得$D_s(s)=\varphi(s)$．

设$a \in K = K^p F(S^*) = F(S^*)$．那么存在$S=\{s_1,\cdots,s_m\} \subseteq S^*$，使得$a \in F(s_1,\cdots,s_m)=F(S)$．令$D_S=\sum_{i=1}^{m} D_{s_i}$．则$D_{s_i}(s_j)=0$，若$i \neq j$，因而$D_S(s_i)=D_{s_i}(s_i)=\varphi(s_i)$，$1 \leqslant i \leqslant m$．如果$S'=\{s'_1,\cdots,s'_n\} \subseteq S^*$，使得$a \in F(S')$，那么令$S''=S \cup S'$，则$D_{S''}|_{F(S)}=D_S$，$D_{S''}|_{F(S')}=D_{S'}$，于是$D_S(a)=D_{S'}(a)=D_{S''}(a)$，这样，定义$D: K \ni a \longmapsto D(a)=D_S(a) \in K$，若$a \in F(S)$，$S=\{s_1,\cdots,s_m\} \subseteq S^*$．则$D(a)$不依赖于$S$的选取，因此$D$是$K$到自身的一个映射．易证$D$是$K$在$F$上一个导子，即$D \in \mathrm{Der}(K/F)$．对于这个$D$来说，我们有$D(s)=\varphi(s)$，$\forall s \in S^*$．所以映射$\mathrm{Der}(K/F) \ni D \longmapsto \varphi_D \in \Phi$是满的．

最后，设$D_1, D_2 \in \mathrm{Der}(K/F)$，而$D_1(s)=D_2(s)$，$\forall s \in S^*$，那么$D_1(a)=D_2(a)$，$\forall a \in K=F(S^*)$，从而$D_1=D_2$．所以上述映射$D \longmapsto \varphi_D$是单的． ▮

推论 4.7.15 设K是域F的一个扩域，$\mathrm{char}F=p>0$，S^*是K在F上一个p-基．如果$|S^*|=n<\infty$，则$\dim_K \mathrm{Der}(K/F)=|S^*|$．

证 令Φ是一切S^*到K的映射所成的集．对于$\varphi, \varphi' \in \Phi$和$a \in K$，定义

$$(\varphi+\varphi')(s)=\varphi(s)+\varphi'(s),$$
$$(a\varphi)(s)=a\varphi(s),$$

$\forall s \in S^*$，易证Φ对于这样定义的运算来说作成K上一个向量空间．

$\theta: \mathrm{Der}(K/F) \ni D \longmapsto \varphi_D \in \Phi$，$\varphi_D(s)=D(s)$，$\forall s \in S^*$，是$K$上向量空间$\mathrm{Der}(K/F)$到$\Phi$的线性映射．于是由4.7.14，$\theta$是$\mathrm{Der}(K/F)$到$\Phi$的同构映射．

对于任意$s\in S^*$. 定义$\sigma_s(s)=1$, $\sigma_s(s')=0$, 若$s'\in S^*\setminus\{s\}$. 则$\{\sigma_s\}_{s\in S^*}$是Φ的一个在K上线性无关的子集.

如果$|S^*|<\infty$, 那么$\{\sigma_s\}_{s\in S^*}$显然是向量空间Φ在K上的一个基. 于是

$$\dim_K \mathrm{Der}(K/F)=\dim_K\Phi=|S^*|. \qquad ▮$$

定理 4.7.16 设K是域F上一个有限生成的扩域. 以下的两个条件是等价的:

(i) K是F上的可分扩域;

(ii) $\dim_K \mathrm{Der}(K/F)=\mathrm{tr.deg}_F K$.

证 (i)$\Longrightarrow$(ii) 因为K/F是有限生成的可分扩张, 所以是可分生成的扩张. 令$x_1,\cdots,x_n$ ($n=\mathrm{tr.deg}_F K$) 是K/F的一个可分超越基, $L=F(x_1,\cdots,x_n)$. 则K/L是可分代数扩张. $F[x_1,\cdots,x_n]$的偏导数$\partial/\partial x_i$ ($1\leqslant i\leqslant n$) 唯一地开拓到商域$L=F(x_1,\cdots,x_n)$上, 是L在F上的导子, 仍以$\partial/\partial x_i$表示, $\partial/\partial x_i\in \mathrm{Der}(L/F)$, $1\leqslant i\leqslant n$. 由4.7.12和4.7.11, $\partial/\partial x_i$可以开拓为K的导子D_i, $D_i\in\mathrm{Der}(K/F)$, $1\leqslant i\leqslant n$.

设$D\in\mathrm{Der}(K/F)$. $D(x_i)=u_i$ ($1\leqslant i\leqslant n$). 令

$$D'=D-\sum_{i=1}^{n}u_iD_i\in\mathrm{Der}(K/F).$$

则$D'(x_i)=0$ ($1\leqslant i\leqslant n$), 于是$D'|_L=0$. 由4.7.11, $D'=0$. 所以$D=\sum_{i=1}^{n}u_iD_i$.

如果$\sum_{i=1}^{n}v_iD_i=0$, $v_i\in K$, 因为$D_i(x_j)=\delta_{ij}$, 所以$v_i=0$ ($1\leqslant i\leqslant n$). 这样, $D_1,\cdots,D_n$是$\mathrm{Der}(K/F)$在K上一个基, 所以$\dim_K(K/F)=\mathrm{tr.deg}_F K$.

(ii)$\Longrightarrow$(i) 如果$\mathrm{char}F=0$, 那么K/F已是可分扩张. 设$\mathrm{char}F=p>0$. 假定$n=\dim_K\mathrm{Der}(K/F)=\mathrm{tr.deg}_F K$. 则

K在F上的p-基含有n个元素.设$s_1,\cdots,s_n$是K在F上一个p-基.令$D_i\in \mathrm{Der}(K/F)$, $D_i(s_j)=\delta_{ij}$. 则$D_1,\cdots,D_n$是$\mathrm{Der}(K/F)$在K上一个基. 于是任意$D\in \mathrm{Der}(K/F)$可以表成$D=\sum_{i=1}^{n} u_iD_i$, 这里$u_i=D(s_i)$, $1\leqslant i\leqslant n$.

令$L=F(s_1,\cdots,s_n)$. 那么对于任意$D\in \mathrm{Der}(K/L)$, 都有$u_i=D(s_i)=0$, $1\leqslant i\leqslant n$, 所以$D=0$. 因此$\mathrm{Der}(K/L)=0$. 因为K是L上有限生成的扩域, 所以根据4.7.11, K是L上可分代数扩域. 我们有

$$\mathrm{tr.deg}_F L=\mathrm{tr.deg}_F K=n.$$

所以$s_1,\cdots,s_n$在F上代数无关. 这样, $s_1,\cdots,s_n$是K在F上一个可分超越基, 所以K/F是可分生成的. 由4.6.1 (i), K是F上可分扩域. ∎

习　题

1. 设R是一个环, A是R的一个子环. D是A到R的一个导子. 证明以下的Leibniz公式:

$$D^k(ab)=\sum_{i=0}^{k}\binom{k}{i}D^i(a)D^{k-i}(b),\quad a,b\in A.$$

2. 设F是一个域, K是F的一个扩域. 对于D_1, $D_2\in \mathrm{Der}(K/F)$, $a\in K$, 定义

$$[D_1,D_2](a)=D_1D_2(a)-D_2D_1(a).$$

(i) 证明$[D_1,D_2]\in \mathrm{Der}(K/F)$, 并且满足以下的Jacobi恒等式: 对于$D_1,D_2,D_3\in \mathrm{Der}(K/F)$,

$$[[D_1,D_2],D_3]+[[D_2,D_3],D_1]+[[D_3,D_1],D_2]=0.$$

(ii) 当$\mathrm{char}F=p>0$时, $D^p\in \mathrm{Der}(K/F)$.

3. 证明, 映射$D: R\to R$是环R的导子必要且只要R到R上2×2矩阵环内的映射

$$a \longmapsto \begin{pmatrix} S & D(a) \\ 0 & a \end{pmatrix}$$

是环同态单射。

4. 设F是一个特征为$p>0$的域，$K=F(\alpha)$，这里$\alpha^{p^2}\in F$但$\alpha^p\notin F$，令$E=F(\alpha^p)$。证明$\{\alpha^p\}$是E在F上一个p-无关子集，但不是K在F上的p-无关子集。

5. 令F是一个特征为$p>0$的域，K是F的一个扩域，B是K在F上一个p-基。证明，对于任意正整数k来说，都有$K=F(K^{p^k}, B)$。

6. 设F是一个特征为$p>0$的域，$K=F(\alpha_1,\cdots,\alpha_n)$。证明以下论断：

(i) 如果$D_1,\cdots,D_r\in \mathrm{Der}(K/F)$是$\mathrm{Der}(K/F)$在$K$上的一个基，那么$s_1,\cdots,s_r\in K$作成$K/F$的一个$p$-基的充要条件是矩阵$(D_i(s_j))_{i,j=1}^r$非退化。

(ii) 如果$s_1,\cdots,s_r\in K$是K/F的一个p-基，那么$D_1,\cdots,D_r\in \mathrm{Der}(K/F)$作成$\mathrm{Der}(K/F)$在$K$上一个基的充要条件是矩阵$(D_i(s_j))_{i,j=1}^r$非退化。

7. 设$K=F(\alpha_1,\cdots,\alpha_n)$是域$F$的一个扩域。证明$K/F$是可分代数扩张的充要条件是存在$n$个多项式$f_1,\cdots,f_n\in F[X_1,\cdots,X_n]$，使得$f_i(\alpha_1,\cdots,\alpha_n)=0\ (1\leqslant i\leqslant n)$，且

$$\det\left(\left(\frac{\partial f_i}{\partial X_j}\right)_\alpha\right)\neq 0,$$

这里$\left(\frac{\partial f_i}{\partial X_j}\right)_\alpha=\frac{\partial f_i(X_1,\cdots,X_n)}{\partial X_j}\Bigg|_{X_k=\alpha_k(1\leqslant k\leqslant n)}$。

第五章　整扩张

我们已经讨论了域的扩张．在这一章里，我们将讨论一下环的扩张．环扩张是交换代数的基本内容之一，它在代数数论和代数几何中都起着重要的作用．

在这一章里，凡是说到环，都指的是有单位元的交换环．说到一个环 R 的子环，都理解为含有 R 的单位元．

5.1　模

设 R 是一个环，M 是一个加法(Abel)群．M 叫做一个**左 R-模**，如果存在一个映射

$$R\times M\ni(r,m)\longmapsto rm\in M,$$

并且下列条件被满足：

(1) $r(m+m')=rm+rm'$，$\forall r\in R$，$m,m'\in M$；

(2) $(r+r')m=rm+r'm$；$(rr')m=r(r'm)$，$\forall r,r'\in R$，$m\in M$．

(3) $1m=m$，$\forall m\in M$．

类似地，交换乘法的次序，可以定义**右 R-模**．由于 R 是交换环，当 M 是一个左 R-模或右 R-模时，我们约定，$rm=mr$，$\forall r\in R$、$m\in M$，则 M 同时成为一个右 R-模或左 R-模。因此，以后我们不再区分左或右 R-模，而统称为 **R-模**，或者称为**环 R 上的模**．

R-模 M 的一个子集 N 叫做 M 的一个**子模**，如果在同样的运算下，N 也作成一个 R-模．

设 N 是 R-模的一个子模．那么商群 M/N 在运算

$$R\times(M/N)\ni(r,m+N)\longmapsto(rm+N)\in M/N$$

之下，也作成一个R-模，称为M对N的**商模**。

环R本身对于环的加法和乘法来说作成一个R-模。这时子模就是R的理想。

设M，N都是R-模。映射φ：$M\longrightarrow N$叫做一个**R-同态**，或者叫做**在R上的同态**，如果

（i） φ是加群M到加群N的群同态；

（ii） $\varphi(rm)=r\varphi(m)$, $\forall r\in R$，$m\in M$。

类似地可以定义模的R-同构。

下面的定理是群和环中有关定理的自然类比。我们只把它叙述出来，而将证明留给读者。

定理 5.1.1 设R是一个环。

（i） 设M是一个R-模，N是M的一个子模。那么加群的自然同态$M\longrightarrow M/N$是一个R-同态。

（ii） 设$\varphi:M\longrightarrow M'$是$R$-模$M$到$R$-模$M'$的一个$R$-同态。则$\mathrm{Ker}\varphi$是$M$的一个子模。如果$N$是$M$的一个子模且$N\subseteq\mathrm{Ker}\varphi$，那么存在唯一的$R$-同态$\varphi':M/N\longrightarrow M'$，使得$\varphi'\circ\pi=\varphi$，这里$\pi$是自然同态$M\longrightarrow M/N$。

（iii） 设N和N'都是R-模M的子模。那么子加群$N+N'$和$N\cap N'$都是子模，并且

$$(N+N')/N'\cong N/(N\cap N').$$

设M是一个环R上的模，$S\subseteq M$。令

$$N=\sum_{s\in S}Rs=\{\sum r_is_i(\text{有限和})\mid r_i\in R,s_i\in S\}.$$

则N是M的一个子模，称为**由S所生成的子模**，N显然是M的包含S的最小子模。子模N说是**有限生成的**，如果N可以由M的一个有限子集生成。$\{0\}$是由空集$\varnothing$生成的。

R-模M的元素$u_1,\cdots$，u_n说是在R上线性相关，如果存在R

中不全为零的元素 $r_i(1\leqslant i\leqslant n)$，使得 $\sum_{i=1}^{n} r_i u_i=0$，否则称为在 R 上**线性无关**. M的一个子集S说是在R上线性无关，如果S的每一个非空有限子集都在R上线性无关.

设M是一个R-模，如果M可以由一个线性无关的子集S在R上生成，那么就称M是一个**自由R-模**，而S叫做M的一个**自由基**.

定理 5.1.2 每一个域F上的模都是自由F-模.

证 设M是一个F-模. 令$\mathfrak{S}$是M的一切线性无关子集所组成的集. 易证$\mathfrak{S}$对于子集的包含关系来说作成一个归纳集. 由Zorn 引理，$\mathfrak{S}$有一个极大元素B. 我们证明，B是M的一个自由基. 为此，只需证明，由B生成的子模N与M相等.

如果不然，那么存在$a\in M$，而$a\notin N$. 由B的极大性可知，$B\cup\{a\}$不再是M的线性无关子集. 于是存在$b_1,\cdots,b_n\in B$，使得$a,b_1,\cdots,b_n$在F上线性相关. 因为F是域，而$b_1,\cdots,b_n$在F上线性无关，所以a可以由$b_1,\cdots,b_n$线性表示，从而$a\in N$. 这与假设矛盾. ∎

由以上定理的证明中可以得出以下

推论 5.1.3 设M是域F上一个模而S是M的一个线性无关子集. 那么存在M的一个自由基B，使得$B\supseteq S$. ∎

设M和N都是环R上的模. 令$\mathrm{Hom}(M,N)$表示一切M到N的R-同态所成的集. 设$\varphi,\varphi'\in\mathrm{Hom}(M,N)$，$r\in R$. 我们定义

$(\varphi+\varphi')(m)=\varphi(m)+\varphi'(m)$；$(r\varphi)(m)=r\varphi(m)$，$\forall\, m\in M$.

则$\mathrm{Hom}(M,N)$对于这样定义的运算来说作成一个R-模.

R-模M的一切子模所成的集$\mathfrak{M}$对于集的包含关系"$\subseteq$"来说作成一个偏序集. 设$\mathfrak{N}$是$\mathfrak{M}$的一个子集. $A\in\mathfrak{N}$叫做$\mathfrak{N}$的一个**极大元素**，如果不存在$B\in\mathfrak{N}$，使得$A\subsetneq B$. 如果$\mathfrak{M}$的每一个非空子集都有极大元素，那么就说，M的子模满足**极大条件**.

R-模M说是满足**升链条件**，如果对于M的任意一个子模的升链

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$$

来说，都存在一个正整数 n，使得$M_m = M_n$，$\forall\, m \geqslant n$。

定理 5.1.4 设M是一个环R上的模．M的子模满足极大条件必要且只要M满足升链条件．

证 设M的子模满足极大条件．令

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$$

是M的任意一个子模升链．那么子模的集$\{M_i \mid i = 1, 2, \cdots\}$有一个极大元素$M_n$。于是$M_n = M_m$，$\forall\, m \geqslant n$。即升链条件成立。

反之，如果M的子模不满足极大条件，那么存在子模所成的非空集$\mathfrak{N}$，$\mathfrak{N}$没有极大元素．取$M_1 \in \mathfrak{N}$，则存在$M_2 \in \mathfrak{N}$，$M_1 \subsetneqq M_2$。对于M_2，存在$M_3 \in \mathfrak{N}$，$M_2 \subsetneqq M_3$。如此继续下去，就得到一个子模的无限升链

$$M_1 \subsetneqq M_2 \subsetneqq \cdots \subsetneqq M_n \subsetneqq \cdots. \qquad \blacksquare$$

习 题

在以下的习题里，R代表一个有单位元1的交换环．

1． 证明定理 5.1.1．

2． 设M，M'是R-模，N，N'分别是M和M'的子模，$f: M \longrightarrow M'$是一个模同态，且$f(N) \subseteq N'$。那么f诱导出商模的同态$\bar{f}: M/N \longrightarrow M'/N'$，$\bar{f}$是模同构必要且只要$f(M) + N' = M'$且$f^{-1}(N') = N$。

3． 设M是一个R-模，N是M的一个子模．证明，在M的包含N的子模所成的集与商模M/N的子模所成的集之间存在一个双射．M/N的子模都有形状P/N，其中P是M的子模且$P \supseteq N$。

4． 设M，N，P都是R-模，且$M \supseteq P$。证明$M \cap (N + P)$

$=(M\cap N)+P$.

5. 设M是一个R-模．由单独一个元素$a\in M$所生成的M的子模叫做循环子模．设$\{M\}_{i\in I}$是M的一个子模族．如果M的每一个元素x都可以唯一地表成$x=\sum_{i\in I}x_i, x_i\in M_i$，并且除去有限个被加项外，其余所有的$X_i$都等于0，那么就称$M$是子模族$\{M_i\}_{i\in I}$的直和，记作$M=\bigoplus_{i\in I}M_i$．证明，对于$M$来说，下列条件等价：

（i） M是一个自由R-模；

（ii） 存在一个非空集X和一个映射$\iota: X\longrightarrow M$，具有以下性质．对于任意一个$R$-模$N$和一个映射$\varphi: X\longrightarrow N$，存在唯一的$R$-模同态$f: M\longrightarrow N$，使得$f\circ\iota=\varphi$．

（iii） M是一族循环子模的直和，每一个循环子模都模同构于R．

6. 举例说明，一个有限生成的R-模作为加群来说不一定是有限生成的．

7. 一个R-模M叫做不可约的，如果除$\{0\}$和M本身以外，不含有其它子模．证明，一个有限生成的R-模M如果满足升链条件，则M可以表示成若干不可约子模的直和．

5.2 Noether 环

设R是一个环．一个R-模M叫做一个Noether模，如果在M中升链条件成立．由5.1.4，这个条件相当于M的子模满足极大条件．

如果R本身是一个Noether R-模，那么就称R是一个**Noether环**．

每一个主理想环都是Noether环．特别，每一个域都是Noether环．

环R本身作为R-模，它的子模就是R的理想，因此，R是一个Noether环当且仅当对于理想来说，极大条件成立；当且仅

当对于R的任意一个理想升链

$$\mathfrak{a}_1\subseteq\mathfrak{a}_2\subseteq\cdots\subseteq\mathfrak{a}_n\subseteq\cdots,$$

都存在一个正整数n，使得$\mathfrak{a}_m=\mathfrak{a}_n$，$\forall m\geqslant n$。

定理 5.2.1 一个环R上的模M是 Noether 模，必要且只要M的每一个子模都是有限生成的。环R是 Noether 环必要且只要R的每一个理想都是有限生成的。

证 显然只需证明第一论断。

设M是一个 Noether R-模。N是M的一个子模。考虑由N的一切有限生成的子模所成的集$\mathfrak{N}$。则$\mathfrak{N}\neq\varnothing$，因为$\{0\}\in\mathfrak{N}$。因为$M$是 Noether 模，所以$\mathfrak{N}$有一个极大元素$N_0$。如果$N_0\subsetneqq N$，那么存在$x\in N$，$x\notin N_0$。于是$N'_0=N_0+Rx$是$N$的一个有限生成的子模，且$N_0\subsetneqq N'_0$。这与$N_0$的极大性相违。因此$N_0=N$，$N$是有限生成的。

反之，设M的每一个子模都是有限生成的。令$N_1\subseteq N_2\subseteq\cdots$是$M$的任意一个子模升链。令$N=\bigcup_{k=1}^{\infty}N_k$。则$N$是$M$的一个子模，因而是有限生成的。设$N=\sum_{i=1}^{n}Rx_i$，$x_i\in N(1\leqslant i\leqslant n)$。则$x_i\in N_{k_i}$，对某一个$k_i$，令$m=\max n_i(1\leqslant i\leqslant r)$。则$x_i\in N_m(1\leqslant i\leqslant n)$，于是$N=N_m$。从而对于任意$r\geqslant m$，都有$N_r=N_m$。所以$M$是一个 Noether 模。 ▮

定理 5.2.2 设M是一个R-模，N是M的一个子模。则M是 Noether 模必要且只要N和M/N都是 Noether 模。

证 令$\varphi: M\longrightarrow M/N$是自然同态。

设M是 Noether 模。令$N_1\subseteq N_2\subseteq\cdots$ $(N_i\in N)$是N的一个子模升链。那么存在m，使得$N_m=N_{m+1}=\cdots$。所以N也是 Noether 模。

又设$\overline{M}_1\subseteq\overline{M}_2\subseteq\cdots$是$M/N$的一个子模升链。令$M_i=$

$\varphi^{-1}(\overline{M}_i)$. 则$M_1\subseteq M_2\subseteq\cdots$是$M$的一个子模升链. 于是存在 m, 使得 $M_m=M_{m+1}=\cdots$. 从而 $\overline{M}_m=\overline{M}_{m+1}=\cdots$. 所以 M/N 是 Noether 模.

反之, 设N和 M/N 都是 Noether 模. 令 $M_1\subseteq M_2\subseteq\cdots$是$M$的一个子模升链. 则

$$M_1\cap N\subseteq M_2\cap N\subseteq\cdots$$

和

$$\varphi(M_1)\subseteq\varphi(M_2)\subseteq\cdots$$

分别是 N 和 M/N 的子模升链. 于是存在 m, 使得 $M_m\cap N=M_{m+1}\cap N=\cdots$, $\varphi(M_m)=\varphi(M_{m+1})=\cdots$. 由此得 $M_m+N=M_{m+1}+N=\cdots$. 于是对于任意 $n\geqslant m$, 有

$$\begin{aligned}M_{n+1}&=M_{n+1}\cap(M_{n+1}+N)=M_{n+1}\cap(M_n+N)\\&=M_n\cap(M_{n+1}+N)=M_n\cap(M_n+N)=M_n.\end{aligned}$$

所以$M_n=M_{n+1}=\cdots$, M 是Noether 模. ∎

定理 5.2.3 Noether 环上有限生成模是 Noether模.

证 设R是一个 Noether 环, M 是一个有限生成 R-模, $u_1,\cdots,u_n$ 是M的一组生成元. 我们对生成元的个数作数学归纳法.

$n=0$ 时是显然的. 设 $n>0$, 并且假设对于可以由 $n-1$ 个元素生成的 R-模来说, 定理成立. 现在设N是M的任意一个子模. 令 $M'=\sum_{i=2}^{n}Ru_i$ 是由 $u_2,\cdots,u_n$ 所生成的子模. 由归纳假设, M' 是 Noether 模. 令

$$\mathfrak{a}=\{a\in R\,|\,au_1\in N+M'\}.$$

则 $\mathfrak{a}$ 是R的一个理想, 因而是由有限个元素生成的. 设 $\mathfrak{a}=(a_1,\cdots,a_s)$. 则 $a_iu_1=v_i+v'_i$, $v_i\in N$, $v'_i\in M'$ $(1\leqslant i\leqslant s)$. 我们断言,

$$N=\sum_{i=1}^{s}Rv_i+N\cap M'.$$

事实上，若$u=\sum_{i=1}^{n}b_iu_i\in N(b_i\in R)$，则$b_1\in\mathfrak{a}$，从而$b_1=\sum_{i=1}^{s}r_ia_i$ $(r_i\in R)$。于是$u-\sum_{i=1}^{s}r_iv_i\in N\cap M'$。所以$u\in\sum_{i=1}^{s}Rv_i+N\cap M'$。这就明了上述断言。

由归纳假设，$N\cap M'$作为Noether模M'的子模，是有限生成的。所以N是有限生成的。于是由5.2.1，M是一个Noether模。 ▮

现在我们来证明以下的定理。

定理 5.2.4 （Hilbert基定理） 设R是一个Noether环，$R[X]$是R上一个不定元X的多项式环。则$R[X]$也是Noether环。

证 假设$R[X]$不是Noether环。那么由5.2.1，存在$R[X]$的一个理想$\mathfrak{a}$，$\mathfrak{a}$不是有限生成的。令$f_1\in\mathfrak{a}$是一个次数最低的多项式。假设$f_k(k\geqslant 1)$已经选出，那么选取f_{k+1}是$\mathfrak{a}\setminus(f_1,\cdots,f_k)$中一个次数最低的多项式，这里$(f_1,\cdots,f_k)$表示$f_1,\cdots,f_k$所生成的$R[X]$的理想。

令$a_k\in R$是f_k的最高次项的系数，$n_k=\deg f_k$ $(k=1,2,\cdots)$。根据f_k的取法，我们有$n_1\leqslant n_2\leqslant\cdots$。并且

$$(a_1)\subseteq(a_1,a_2)\subseteq\cdots\subseteq(a_1,\cdots,a_k)\subseteq\cdots$$

是R的一个理想升链。因为R是Noether环，所以存在k，使得$(a_1,\cdots,a_k)=(a_1,\cdots,a_{k+1})$。于是

$$a_{k+1}=\sum_{i=1}^{k}r_ia_i,\quad r_i\in R.$$

这样一来，

$$g=f_{k+1}-\sum_{i=1}^{k}r_iX^{n_{k+1}-n_i}f_i\in I\setminus(f_1,\cdots,f_k),$$

并且$\deg g<\deg f_{k+1}$。这与f_{k+1}的取法矛盾。 ▮

由这个定理我们可以得出一系列重要的推论。

推论 5.2.5 一个 Noether 环 R 上 n 个不定元的多项式环 $R[X_1, \cdots, X_n]$ 也是 Noether 环. 特别，一个域 F 上 n 个不定元的多项式环 $F[X_1, \cdots, X_n]$ 是 Noether 环。 ▌

推论 5.2.6 一个 Noether 环 R 上由有限个元素 $a_1, \cdots, a_n$ 生成的交换环 $R[a_1, \cdots, a_n]$ 是 Noether 环.

证 φ: $R[X_1, \cdots, X_n] \longrightarrow R[a_1, \cdots, a_n]$, $\varphi(X_i) = a_i$ $(1 \leqslant i \leqslant n)$ 是一个 R-模同态，$R[a_1, \cdots, a_n] \cong R[X_1, \cdots, X_n]/\mathrm{Ker}\varphi$. 由 5.2.2，$R[a, \cdots, a_n]$是 Noether环. ▌

推论 5.2.7 一个域 F 上有限生成的交换环是 Noether 环。 ▌

定理 5.2.8 设 $A \subseteq B \subseteq C$ 是环的一个序列，并且下列三个条件被满足：

(i) A是 Noether环；

(ii) C是A上有限个元素生成的环；

(iii) C是有限生成的 B-模；

那么B作为环，是A上有限个元素生成的。

证 由(ii)，存在$x_1, \cdots, x_m \in C$，使得 $C = A[x_1, \cdots, x_m]$. 又由(iii)，存在 $y_1, \cdots, y_n \in C$，使得 $C = \sum_{i=1}^{n} By_i$. 我们有

(1) $$x_i = \sum_{j=1}^{n} b_{ij} y_j, \quad b_{ij} \in B, \quad 1 \leqslant i \leqslant m.$$

(2) $$y_p y_q = \sum_{r=1}^{n} b_{pqr} y_r, \quad b_{pqr} \in B, \quad 1 \leqslant p, q \leqslant m.$$

一切b_{ij}和b_{pqr} $(1 \leqslant i \leqslant m, 1 \leqslant j, p, q, r \leqslant n)$ 在A上生成B的一个子环B_0.

$$A \subseteq B_0 = A[\cdots, b_{ij}, \cdots, \cdots, b_{pqr}, \cdots] \subseteq B.$$

由(i)，A是 Noether 环，所以由 5.2.5，B_0也是 Noether 环。

C的任意元素 z 可以表成$z=f(x_1,\cdots,x_n)$的形式，$f\in A[X_1,\cdots,X_n]$。把 x_i 的表示式(1)代入，反复利用(2)，可知 $z\in\sum_{i=1}^{n}B_0y_i$。所以$C=\sum_{i=1}^{n}B_0y_i$。因此，C是一个有限生成的B_0-模。因为B_0是 Noether 环，所以由 5.2.3，C是一个Noether B_0-模。B是C的一个子B_0-模，所以B是有限生成的B_0-模。因此，B是B_0上由有限个元素生成的环。又 B_0是A上由有限个元素生成的环。所以B是A上由有限个元素生成的环。 ∎

定理 5.2.9 设F是一个域。$B=F[x_1,\cdots,x_n]$是有限个元素 $x_1,\cdots,x_n$ 在F上生成的环。如果B是域，则B是F上有限次代数扩域。

证 设$B=F[x_1,\cdots,x_n]$ 是域，我们证明，B是F的代数扩域，从而是F的有限次扩域。

如果B/F不是代数域扩张，那么适当编号，可以假设 $x_1,\cdots,x_r(r\geqslant1)$ 在F上代数无关，而$x_{r+1},\cdots,x_n$在$E=F(x_1,\cdots,x_r)$ 上是代数的。于是B是E上有限次代数扩域，从而B是有限生成的E-模。我们有$F\subseteq E\subseteq B$，于是由 5.2.8，E作为环，是由有限个元素$y_1,\cdots,y_s$在F上生成的：$E=F[y_1,\cdots,y_s]$，$y_i\in E=F(x_1,\cdots,x_r)$，所以

$$y_i=f_i(x_1,\cdots,x_r)/g_i(x_1,\cdots,x_r),\quad f_i,g_i\in E[x_1,\cdots,x_r].$$

多项式环 $F[x_1,\cdots,x_r]$ 含有无限多个不可约多项式。因此存在一个不可约多项式 $p=p(x_1,\cdots,x_r)\in F[x_1,\cdots,x_r]$，使得 p 不能整除每一个 $g_i(1\leqslant i\leqslant s)$。

另一方面，$1/p\in E=F[y_1,\cdots,y_s]$。所以

$$\frac{1}{p}=\sum a_{i_1,\cdots,i_s}y_1^{i_1}\cdots y_s^{i_s},\quad a_{i_1,\cdots,i_s}\in F.$$

将 $y_i=f_i/g_i$ 代入上式的右端，然后两端同乘以 p 和右端各项的公分母，我们得到

$$g_1(x_1,\cdots,x_r)^{k_1}\cdots g_s(x_1,\cdots,x_r)^{k_s}=p(x_1,\cdots,x_r)h(x_1,\cdots,x_r),$$

这里 $h(x_1,\cdots,x_r)\in F[x_1,\cdots,x_r]$. 由于 $F[x_1,\cdots,x_r]$是唯一因式分解整环，所以 p 一定整除某一个 g_i. 这就导致矛盾. 这样一来,必须 $x_1,\cdots,x_r$都是F上的代数元,从而B是F的代数扩域. ▮

由 5.2.9 立即得到以下

推论 5.2.10 设F是一个域，$B=F[x_1,\cdots,x_n]$是有限个元素在F上生成的环,$\mathfrak{m}$是B的一个极大理想. 那么域$B/\mathfrak{m}$是F上的有限次代数扩域. 特别,如果F是代数闭域,那么$B/\mathfrak{m}\cong F$. ▮

注 5.2.10 通常称为Hilbert零点定理的弱形式（参看5.8.5）.

习　题

在以下的习题里，R代表一个有单位元的交换环.

1. R的元素a说是不可约的，如果$a\neq 0$又不是可逆元素，并且不能写成两个非可逆元素的积. 证明，如果R是Noether环，则R中每一个既非零又非可逆的元素都可以写成若干个不可约元素的乘积.

2. 令

$$\mathfrak{n}=\{a\in R\mid a^n=0\text{ 对某个}n>0\}$$

是R中一切幂零元素所组成的集，则$\mathfrak{n}$是R的一个理想，称为R的**幂零元素根**，R的一个理想$\mathfrak{a}$说是幂零的，如果存在正整数n使得$\mathfrak{a}^n=\{0\}$. 证明，如果R是Noether环，则R的幂零元素根一定是幂零理想.

3. 设$\mathfrak{a}$是R的一个有限生成的理想，N是R-模M的一个子模. 如果对于每一个$a\in\mathfrak{a}$，都有一个正整数m(依赖于a)，使得$a^mM\subseteq N$，则存在一个正整数n，使$\mathfrak{a}^nM\subseteq N$.

4. 令$R[[X]]=\{(a_0,a_1,a_2,\cdots)\mid a_i\in R\}$是$R$的元素所组成的一切无穷序列的集. 在$R[[X]]$中如下地定义加法和乘法：

$$(a_0,a_1,a_2,\cdots)+(b_0,b_1,b_2,\cdots)=(a_0+b_0,a_1+b_1,a_2+b_2,\cdots)$$

$$(a_0, a_1, a_2, \cdots)(b_0, b_1, b_2, \cdots) = (c_0, c_1, c_2, \cdots) ,$$

其中$c_k = \sum_{i+j=k} a_i b_j$，则$R[[X]]$作成一个有单位元的交换环．通过同态单射$R \in a \longmapsto (a, 0, 0, \cdots) \in R[[X]]$，$R$被嵌入$R[[X]]$。令$X = (0, 1, 0, \cdots)$。则$R[[X]]$的元素可以唯一地写成$\sum_{i=0}^{\infty} a_i X^i$的形式。

证明，如果R是Noether环，则$R[[X]]$也是Noether环。

5.3 交换环的一些理想

交换环的理想论是交换代数的基本内容之一．我们不准备详细讨论这个内容．只介绍在今后讨论中要用到的一些概念．

仍设R是一个有单位元的交换环．

R的一个理想$\mathfrak{p}$叫做一个素理想，如果$\mathfrak{p} \neq R$，并且满足以下的条件：

$$a, b \in R,\ ab \in \mathfrak{p} \Longrightarrow a \in \mathfrak{p} \text{ 或 } b \in \mathfrak{p} .$$

定理 5.3.1 设$\mathfrak{p}$是环R的一个理想，且$\mathfrak{p} \neq R$．以下四个条件是等价的：

(i) $\mathfrak{p}$是一个素理想；

(ii) $\mathfrak{a}$，$\mathfrak{b}$是R的理想，且$\mathfrak{a}\ \mathfrak{b} \subseteq \mathfrak{p} \Longrightarrow \mathfrak{a} \subseteq \mathfrak{p}$或$\mathfrak{b} \subseteq \mathfrak{p}$；

(iii) $\mathfrak{a}$，$\mathfrak{b}$是R的理想，且$\mathfrak{a} \not\subseteq \mathfrak{p}$，$\mathfrak{b} \not\subseteq \mathfrak{p} \Longrightarrow \mathfrak{a}\ \mathfrak{b} \not\subseteq \mathfrak{p}$；

(iv) 剩余类环$R/\mathfrak{p}$是整环。

证 (i)$\Longrightarrow$(ii) 设$\mathfrak{a} \not\subseteq \mathfrak{p}$，那么存在$a \in \mathfrak{a}$但$a \notin \mathfrak{p}$．于是对于任意$b \in \mathfrak{b}$来说，都有$ab \in \mathfrak{p}$，从而$b \in \mathfrak{p}$．

(ii)$\Longrightarrow$(iii) 显然．

(iii)$\Longrightarrow$(iv) 令 $\bar{a} = a + \mathfrak{p}$表示在自然同态$R \longrightarrow R/\mathfrak{p}$之下，$R$的元素$a$在$R/\mathfrak{p}$中的象．如果$\bar{a}$是$R/\mathfrak{p}$的一个零因子，则$\bar{a} \neq \bar{0}$，并且存在$b \in R$，使得$\bar{b} \neq \bar{0}$，而$\bar{a}\ \bar{b} = \bar{0}$（即$ab \in \mathfrak{p}$）。

令 $\mathfrak{a}=Ra+\mathfrak{p}$，$\mathfrak{b}=Rb+\mathfrak{p}$；则 $\mathfrak{a}$，$\mathfrak{b}$ 都是 R 的理想，且 $\mathfrak{a}\not\subseteq\mathfrak{p}$，$\mathfrak{b}\not\subseteq\mathfrak{p}$。于是由(iii)，$\mathfrak{a}\mathfrak{b}\not\subseteq\mathfrak{p}$。这与 $ab\in\mathfrak{p}$ 的假设矛盾。因此 $R/\mathfrak{p}$ 没有非零的零因子。

(iv)$\Longrightarrow$(i) 显然。 ▮

下面的定理可以说明素理想的存在。

环 R 的一个非空子集 S 叫做一个**乘法闭子集**，如果

$$a,b\in S\Longrightarrow ab\in S.$$

例如，R 的一切可逆元素所成的集是一个乘法闭子集。

定理 5.3.2 设 S 是环 R 的一个乘法闭子集。$\mathfrak{a}$ 是 R 的一个理想，且 $\mathfrak{a}\cap S=\varnothing$。令 $\mathfrak{S}$ 是 R 中一切与 S 不相交的理想所成的集。则 $\mathfrak{S}$ 对于集的包含关系来说有一个极大元素。$\mathfrak{S}$ 的每一个极大元素都是 R 的素理想。

证 容易证明，$\mathfrak{S}$ 是一个归纳集。由Zorn 引理，$\mathfrak{S}$ 有一个极大元素。

设 $\mathfrak{p}$ 是 $\mathfrak{S}$ 的一个极大元素。如果 $\mathfrak{a}$，$\mathfrak{b}$ 是 R 的理想，且 $\mathfrak{a}\not\subseteq\mathfrak{p}$，$\mathfrak{b}\not\subseteq\mathfrak{p}$，那么由 $\mathfrak{p}$ 的极大性，$\mathfrak{a}\cap S$ 和 $\mathfrak{b}\cap S$ 分别含有元素 a 和 b。于是 $ab\in S$。$ab\in\mathfrak{a}\mathfrak{b}$，而 $ab\notin\mathfrak{p}$，所以 $\mathfrak{a}\mathfrak{b}\not\subseteq\mathfrak{p}$。由 5.3.1 (iii)，$\mathfrak{p}$ 是素理想。 ▮

如果 S 只含有可逆元素，那么上述定理中极大元素就是 R 的极大理想。

现在设 $\mathfrak{a}$ 是环 R 的一个理想。R 的子集

$$\{r\in R\,|\,r^n\in\mathfrak{a}，对某个\ n\}$$

叫做 $\mathfrak{a}$ **的根**，记作 $\sqrt{\mathfrak{a}}$。显然 $\mathfrak{a}\subseteq\sqrt{\mathfrak{a}}$。容易直接证明，$\sqrt{\mathfrak{a}}$ 是 R 的理想。然而由以下定理，也可以证明 $\sqrt{\mathfrak{a}}$ 是理想。

定理 5.3.3 设 $\mathfrak{a}$ 是环 R 的一个理想。那么 $\mathfrak{a}$ 的根 $\sqrt{\mathfrak{a}}$ 等于 R 的一切包含 $\mathfrak{a}$ 的素理想的交。

如果 R 是一个 Noether 环，则存在一个正整数 m，使得 $(\sqrt{\mathfrak{a}})^m\subseteq\mathfrak{a}$。

证 设 $a\in\sqrt{\mathfrak{a}}$，而 $\mathfrak{p}$ 是任意一个包含 $\mathfrak{a}$ 的素理想．则 $a^m\in\mathfrak{a}\subseteq\mathfrak{p}$ 对某个 m．从而 $a\in\mathfrak{p}$．

反之．设 $b\in R$，而 $b\notin\sqrt{\mathfrak{a}}$．令 $S=\{b^n\mid n\geqslant 0\}$．则 S 是一个乘法闭子集，且 $\mathfrak{a}\cap S=\varnothing$．于是由 5.3.2，存在一个素理想 $\mathfrak{p}\supseteq\mathfrak{a}$，且 $\mathfrak{p}\not\ni b$．

如果 R 是 Noether 环，那么 $\sqrt{\mathfrak{a}}$ 由有限个元素生成．设 $\sqrt{\mathfrak{a}}=(a_1,\cdots,a_s)$．则 $a_i^{n_i}\in\mathfrak{a}$，对某个 $n_i(1\leqslant i\leqslant s)$．令 $m=\sum_{i=1}^{s}n_i$．则 $(\sqrt{\mathfrak{a}})^m\subseteq\mathfrak{a}$． ∎

习　题

1. （孙子定理）设 R 是一个有单位元的交换环，$\mathfrak{a}_1,\cdots,\mathfrak{a}_n$ 是 R 的理想，且 $\mathfrak{a}_i+\mathfrak{a}_j=R$，若 $i\neq j$．那么对于任意给定的 $b_1,\cdots,b_n\in R$，总存在 $b\in R$，使得

$$b\equiv b_i(\mathrm{mod}\ \mathfrak{a}_i),\quad 1\leqslant i\leqslant n.$$

如果 $c\in R$，使得

$$c\equiv b_i(\mathrm{mod}\ \mathfrak{a}_i),\quad 1\leqslant i\leqslant n,$$

那么 $b\equiv c(\mathrm{mod}\ \mathfrak{a}_1\cap\cdots\cap\mathfrak{a}_n)$．

2. 设 $f(X)$ 是复数域 C 上一个次数大于零的多项式，$a_1,\cdots,a_r\in C$ 是 $f(X)$ 一切两两不同的根．证明，存在一个没有常数项的多项式 $p(X)\in C[X]$，使得

$$p(X)\equiv a_i(\mathrm{mod}(X-a_i)^{m_i})1\leqslant i\leqslant r.$$

3. 一个 n 阶方阵 A 叫做半单的．如果它的最小多项式没有重根；A 叫做幂零的，如果存在正整数 m 使得 $A^m=0$，证明，对于复数域上每一个 n 阶方阵 A，总存在一个半单矩阵 D 和一个幂零矩阵 N，它们都是 A 的没有常数项的多项式，使得 (i) $A=D+N$；(ii) $DN=ND$．满足条件(i)和(ii)的半单矩阵和幂零矩阵是由 A 唯一确定的（矩阵的Jordan分解）．

4. 设F是一个域，R是F上一个有限生成的交换环，$\mathfrak{a}$是R的一个理想。令$J(\mathfrak{a})$表示R的一切包含$\mathfrak{a}$的极大理想的交。证明：$J(\mathfrak{a})=\sqrt{\mathfrak{a}}$。

5. 令R是一个有单位元的交换环。

(i) 设$\mathfrak{p}_1,\cdots,\mathfrak{p}_r$是素理想，$\mathfrak{a}$是一个理想且$\mathfrak{a}\subseteq\bigcup_{i=1}^{r}\mathfrak{p}_i$。则$\mathfrak{a}\subseteq\mathfrak{p}_i$对某一个$i$。

(ii) 设$\mathfrak{a}_1,\cdots,\mathfrak{a}_r$是$R$的理想，$\mathfrak{p}$是一个素理想且$\mathfrak{p}\supseteq\bigcap_{i=1}^{r}\mathfrak{a}_i$。则$\mathfrak{p}\supseteq\mathfrak{a}_i$对某一个$i$。如果$\mathfrak{p}=\bigcap_{i=1}^{r}\mathfrak{a}_i$，则$\mathfrak{p}=\mathfrak{a}_i$对某一个$i$。

6. 设R是一个有单位元的交换环，$\mathfrak{a}$，$\mathfrak{b}$是R的理想。定义

$$(\mathfrak{a}:\mathfrak{b})=\{x\in R\mid x\,\mathfrak{b}\subseteq\mathfrak{a}\}.$$

称为$\mathfrak{a}$与$\mathfrak{b}$的商。证明：

(i) $(\mathfrak{a}:\mathfrak{b})$是理想；

(ii) $\mathfrak{a}\subseteq(\mathfrak{a}:\mathfrak{b})$；

(iii) $(\mathfrak{a}:\mathfrak{c})\mathfrak{c}\subseteq\mathfrak{a}$；

(iv) $((\mathfrak{a}:\mathfrak{b}):\mathfrak{c})=(\mathfrak{a}:\mathfrak{b}\mathfrak{c})=((\mathfrak{a}:\mathfrak{c}):\mathfrak{b})$；

(v) $\left(\bigcap_{i\in I}\mathfrak{a}_i:\mathfrak{b}\right)=\bigcap_{i\in I}(\mathfrak{a}_i:\mathfrak{b})$；

(vi) $\left(\mathfrak{a}:\sum_{i=1}^{n}\mathfrak{b}_i\right)=\bigcap_{i=1}^{n}(\mathfrak{a}:\mathfrak{b}_i)$。

7. 证明：一个有单位元的交换环R是Noether环必要且只要R的每一个素理想都是有限生成的。

5.4 局部化

在这一节里，我们将介绍交换代数中一个非常有用的概念，这就是局部化的概念。

环的局部化正是我们所熟悉的从一个整环来构造商域过程的推广．

设 R 是一个环．S 是 R 的一个乘法闭子集，并且 $0 \notin S$．考虑一切元素对 (a, s) 所成的集

$$Q = \{(a,s) \mid a \in R, s \in S\}.$$

在 Q 中如下地定义一个关系：对于 $(a,s),(a',s') \in Q$，定义

$$(a,s) \sim (a',s') \Longleftrightarrow \text{存在 } t \in S, \text{使得 } t(s'a - sa') = 0.$$

直接验证可知，$\sim$ 是 Q 的一个等价关系．由此决定 Q 的一个分类．令 a/s 表示 (a,s) 所在的类．一切类所成的集记作 $S^{-1}R$．

我们将在 $S^{-1}R$ 内定义加法和乘法，使 $S^{-1}R$ 作成一个有单位元的交换环．

首先定义加法：

$$\frac{a}{s} + \frac{a'}{s'} = \frac{s'a + sa'}{ss'}.$$

我们证明，这个定义不依赖于代表的选取．设 $a_1/s_1 = a/s$，$a'_1/s'_1 = a'/s'$．那么存在 $t, u \in S$，使得

$$t(sa_1 - s_1 a) = 0, \quad u(s'a'_1 - s'_1 a') = 0.$$

把第一个等式乘以 $us's'_1$，把第二个等式乘以 tss_1，然后相加，我们得到

$$tu(s's'_1(sa_1 - s_1 a) + ss_1(s'a'_1 - s'_1 a')) = 0.$$

或

$$tu(ss'(s'_1 a_1 + s_1 a'_1) - s_1 s'_1(s'a + sa')) = 0.$$

所以

$$(s'_1 a + s_1 a'_1, s_1 s'_1) \sim (s'a + sa', ss').$$

即

$$\frac{s'_1 a_1 + s_1 a'_1}{s_1 s'_1} = \frac{s'a + sa'}{ss'}.$$

容易验证，这样定义的加法满足结合律和交换律．显然有

$s'a/s's=a/s$。于是

$$\frac{0}{s'}+\frac{a}{s}=\frac{s'a}{s's}=\frac{a}{s}.$$

所以 $0/s'$ 是零元．又

$$\frac{a}{s}+\frac{-a}{s}=\frac{0}{s^2}.$$

所以 $-a/s$ 是 a/s 的负元．这样，$S^{-1}A$ 对于以上定义的加法来说作成一个加群．

现在定义乘法：

$$\left(\frac{a}{s}\right)\left(\frac{a'}{s'}\right)=\frac{aa'}{ss'}.$$

易证这个定义也不依赖于代表的选取，并且这个乘法满足结合律和交换律，加法与乘法被分配律联系着．$s/s(s\in S)$ 显然是 $S^{-1}R$ 的单位元．

这样，$S^{-1}R$ 作成一个有单位元的交换环．称为**R对于S的分式环**．

对于R的每一个元素a，类 sa/s 不依赖于 $s\in S$ 的选取．因此

$$\psi:\ R\ni a\longrightarrow sa/s\in S^{-1}R$$

是R到 $S^{-1}R$ 的一个映射．ψ是一个环同态，并且把 R 的单位元映成 $S^{-1}R$ 的单位元．ψ称为R到 $S^{-1}R$ 的**自然同态**．

由以上构造过程可知，如果R是一个整环，$S=R\setminus\{0\}$．则 $S^{-1}R$ 就是R的商域．

一般，如果R是一个整环，而S是R的一个乘法闭子集且 $S\not\ni 0$，那么自然同态ψ：$R\to S^{-1}R$是单射．事实上，如果 $a\in R$，而 $sa/s=0/s'$，则$ss'a=0$，因为$s,s'\neq 0$，所以 $a=0$．这时我们可以把$\psi(R)$与R等同起来，而把R看成 $S^{-1}R$ 的一个子环．

对于$r\in R$，$a/s\in S^{-1}R$，定义 $r(a/s)=ra/s$，则 $S^{-1}R$

作成一个R-模。

如下构成的分式环特别重要。

设R是一个环，$\mathfrak{p}$是R的一个素理想。令$S=R\setminus\mathfrak{p}$。由素理想的定义知S是R的一个乘法闭子集，且$0\notin S$。这时分式环$S^{-1}R$叫做**R对$\mathfrak{p}$的分式环**并且记作$R_{\mathfrak{p}}$。

一个环R叫做一个**局部环**，如果R有唯一的极大理想。

设R是一个局部环，$\mathfrak{m}$是R的唯一的极大理想。如果$a\in R$但$a\notin\mathfrak{m}$，则a是R的一个可逆元素。因为不然的话，a生成R的一个真理想(a)。由于$\mathfrak{m}$是R的唯一的极大理想，所以$(a)\subseteq\mathfrak{m}$，这就导致矛盾。

定理 5.4.1 设R是一个环，$\mathfrak{p}$是R的一个素理想。R对于$\mathfrak{p}$的分式环$R_{\mathfrak{p}}$是一个局部环。

证 令

$$\mathfrak{m}=\mathfrak{p}R_{\mathfrak{p}}=\{p/s\mid p\in\mathfrak{p},s\in R\setminus\mathfrak{p}\}.$$

易证$\mathfrak{m}$是$R_{\mathfrak{p}}$的一个理想。设$\mathfrak{a}$是$R_{\mathfrak{p}}$的一个理想。如果$\mathfrak{a}\not\subseteq\mathfrak{m}$，则$\mathfrak{a}$必含有一个形如$s'/s$的元素，$s,s'\notin\mathfrak{p}$。于是$s'/s$在$R_{\mathfrak{p}}$中有逆元$s/s'$。所以$\mathfrak{a}=R_{\mathfrak{p}}$。这就证明了$\mathfrak{m}$是$R_{\mathfrak{p}}$中唯一的极大理想，所以$R_{\mathfrak{p}}$是局部环。 ∎

从环R过渡到$R_{\mathfrak{p}}$的过程叫做**R在$\mathfrak{p}$的局部化**。

习　题

以下说到环都指的是有单位元的交换环。环同态$f: R\longrightarrow R'$都要求R的单位元映成R'的单位元。

1. 设$f: R\longrightarrow R'$是环同态，S是R的一个乘法闭子集，并且对于任意$s\in S$，$f(s)$都是R'的可逆元素。证明，存在唯一的环同态$\varphi: S^{-1}R\longrightarrow R'$，使得$f=\varphi\circ\psi$，这里$\psi: R\longrightarrow S^{-1}R$是自然同态。

2. 设S和T是R的两个乘法闭子集，U是T在自然同态

$R \longrightarrow S^{-1}R$ 之下的象，证明，环$(ST)^{-1}R$ 与 $U^{-1}(S^{-1}R)$同构。

3. （i）设$\mathbf{Z}$是整数环，p是一个素数、$\mathfrak{p}=(p)$。$\mathbf{Z}_{\mathfrak{p}}=?$

（ii）设$f \in R, f \neq 0$，令$S=\{f^n \mid n>0\}$。记$S^{-1}R=R_f$。

如果$R=\mathbf{Z}$，$f \in R$，$f \neq 0$，$R_f=?$

4. 设S是环R的一乘法闭子集，$\mathfrak{a}$是R的一个理想。令

$$S^{-1}\mathfrak{a}=\{a/s \mid a \in \mathfrak{a},\ s \in S\}.$$

（i）证明，$S^{-1}\mathfrak{a}$是$S^{-1}R$的一个理想，称为$\mathfrak{a}$在$S^{-1}R$中的扩张。

（ii）设$\mathfrak{a}$，$\mathfrak{b}$是R的理想．证明

(*a*) $S^{-1}(\mathfrak{a}+\mathfrak{b})=S^{-1}\mathfrak{a}+S^{-1}\mathfrak{b}$；

(*b*) $S^{-1}(\mathfrak{a}\mathfrak{b})=(S^{-1}\mathfrak{a})(S^{-1}\mathfrak{b})$；

(*c*) $S^{-1}(\mathfrak{a} \cap \mathfrak{b})=S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{b}$。

（iii）$S^{-1}\mathfrak{a}=S^{-1}R \Longleftrightarrow S \cap \mathfrak{a}=\varnothing$。

5. 设$\mathfrak{a}$是R的一个理想，$S=1+\mathfrak{a}$。证明，S是R的一个乘法闭子集，并且$S^{-1}\mathfrak{a}$包含在$S^{-1}R$的每一个极大理想内。

6. 设S是R的一个乘法闭子集．$\psi: R \longrightarrow S^{-1}R$是自然同态。$\mathfrak{b}$是$S^{-1}R$的一个理想，则$\psi^{-1}(\mathfrak{b})$是$R$的一个理想，称为$\mathfrak{b}$在$R$中的局限．证明：

（i）如果$\mathfrak{a}$是R的一个理想，则；$\mathfrak{a} \subseteq \psi^{-1}(S^{-1}\mathfrak{a})$；

（ii）如果$\mathfrak{b}$是$S^{-1}R$的一个理想，则

$$S^{-1}(\psi^{-1}(\mathfrak{b}))=\mathfrak{b}.$$

（iii）如果$\mathfrak{p}$是R的一个素理想且$S \cap \mathfrak{p}=\varnothing$，则$S^{-1}\mathfrak{p}$是$S^{-1}R$的一个素理想且$\psi^{-1}(S^{-1}\mathfrak{p})=\mathfrak{p}$。

（iv）R中一切与S不相交的素理想所组成的集与$S^{-1}R$中一切素理想所组成的集之间存在双射。

7. 证明，R是局部环的充分且必要条件是对于任意$a, b \in R$，若$a+b=1$，则a或b是可逆元素。

8. 证明下列条件对于R来说是等价的：

（i） R是一个局部环；

（ii） R的一切非可逆元素都含在某一个理想$\mathfrak{m}\neq R$内；

（iii） R的一切非可逆元素作成一个理想。

9. 设$\mathfrak{m}$是R的一个极大理想，n是一个正整数。证明，剩余类环$R/\mathfrak{m}^n$是局部环。

10. 证明，局部环的任意非零同态象也是局部环。

11. 设R是一个Noether环，S是R的一个乘法闭子集。则$S^{-1}R$也是Noether环。

5.5 整扩张

设R是一个环，A是R的一个子环。正如本章一开始就假定的那样，A含有R的单位元。

R的一个元素x说是**A上的整元**，或者说，**x在A上是整的**，如果存在一个系数在A内且最高次项系数是1的非零多项式。

$$f(X)=X^n+a_1X^{n-1}+\cdots+a_n\in A[X],$$

使得$f(x)=0$。

一个环R上的模M说是**忠实的**，如果$a\in R$，使得$aM=0$，则$a=0$。因为R有单位元，所以环R作为R-模，是忠实的。

定理 5.5.1 设R是一个环，A是R的一个子环。对于R的元素x来说，下列四个条件是等价的：

（i） x在A上是整的；

（ii） A上由x所生成的子环$A[x]$是一个有限生成的A-模；

（iii） 存在R的一个子环B，$B\ni x$且B是有限生成的A-模。

（iv） 存在一个忠实的$A[x]$-模M，且M是一个有限生成的A-模。

证 (i)$\Longrightarrow$(ii) 设

$$x^n+a_1x^{n-1}+\cdots+a_n=0 \quad (a_i\in A,\ 1\leqslant i\leqslant n).$$

那么对于任意 $r\geqslant 0$，都有

$$x^{n+r}=-(a_1x^{n+r-1}+\cdots+a_nx^r).$$

所以 $A[x]=A+Ax+\cdots+Ax^{n-1}$ 是由 $1,x,\cdots,x^{n-1}$ 所生成的 A-模。

(ii)⟹(iii) 取 $B=A[x]$ 即可。

(iii)⟹(iv) 取 $M=B$。则 M 是一个忠实 $A[x]$-模。又由(iii)，M 是一个有限生成 A-模。

(iv)⟹(i) M 是一个有限生成 A-模。令 $u_1,\cdots,u_n$ 是它的一组生成元。因为 $A[x]M\subseteq M$，所以 $xM\subseteq M$。设

$$xu_i=\sum_{j=1}^{n}a_{ij}u_j,\ a_{ij}\in A,\ 1\leqslant i\leqslant n,$$

那么

$$\sum_{j=1}^{n}(\delta_{ij}x-a_{ij})u_j=0,\ 1\leqslant i\leqslant n,$$

这里 $\delta_{ij}=1$，若 $i=j$，$\delta_{ij}=0$，若 $i\neq j$。令

$$D=\begin{pmatrix} x-a_{11} & -a_{12} & \cdots & -a_{1n}\\ -a_{21} & x-a_{22} & \cdots & -a_{2n}\\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots\\ -a_{n1} & -a_{n2} & \cdots & x-a_{nn}\end{pmatrix}.$$

那么上面的方程可以写成

$$D\begin{pmatrix}u_1\\u_2\\ \vdots\\u_n\end{pmatrix}=\begin{pmatrix}0\\0\\ \vdots\\0\end{pmatrix}.$$

两边乘以 D 的伴随矩阵 D^* 得

$$\det D\cdot u_k=0,\ 1\leqslant k\leqslant n.$$

所以 $\det D\in A[x]$ 零化 M，即 $\det DM=0$。因为 M 是一个忠

实 $A[x]$-模，所以 $\det D=0$. 展开这个行列式就得到

$$x^n+a_1x^{n-1}+\cdots+a_n=0,\ a_i\in A(1\leqslant i\leqslant n).$$

所以 x 在 A 上是整的。 ∎

由这个定理可以得出一系列重要的推论。

推论 5.5.2 设 $x_1,\cdots,x_n\in R$ 在 A 上是整的，那么 $A[x_1,\cdots,x_n]$是一个有限生成的 A-模。

证 对 n 作数学归纳法。记 $A_r=A[x_1,\cdots,x_r]$。设 A_{n-1} 是有限生成 A-模。由 5.5.1，$A_n=A_{n-1}[x_n]$ 是有限生成 A_{n-1}-模。所以也是有限生成的 A-模。 ∎

推论 5.5.3 R 中一切在 A 上的整元所组成的集是 R 的一个子环。

证 令 C 是 R 中一切在 A 上的整元所成的集，设 $x,y\in C$。由 5.5.2，$A[x,y]$是有限生成的 A-模。$x-y,xy\in A[x,y]$，由5.5.1 (iii)，$x-y,xy\in C$。 ∎

环 R 中在子环 A 上的整元的全体所成的环 C 叫做 A 在 R 内的**整闭包**。如果 $C=A$，则称 A 是在 R 中**整闭的**。如果 $C=R$，则称**R 在 A 上是整的**。在最后情形称 R 为 A 上的**整扩环**。

推论 5.5.4 设 $x_1,\cdots,x_n\in R$ 是 A 上的整元。则 $A[x_1,\cdots,x_n]$是 A 上的整扩环。

证 设 $x\in A[x_1,\cdots,x_n]$。由 5.5.2及5.5.1 (iii)，x 是 A 上的整元。 ∎

推论 5.5.5 设 A 和 B 都是环 R 的子环，且 $A\subseteq B\subseteq R$。如果 B 是 A 上的整扩环，R 是 B 上的整扩环，则 R 是 A 上的整扩环。

证 设 $z\in R$。假定

$$z^n+b_1z^{n-1}+\cdots+b_n=0,\ b_i\in B(1\leqslant i\leqslant n).$$

令 $B'=A[b_1,\cdots,b_n]\subseteq B$。则 z 是 B' 上的整元。所以 $B'[z]$ 是有限生成的 B'-模。又由 5.5.2，B' 是有限生成的 A-模。所以

$B'[z]$也是有限生成的 A-模. $z\in B'[z]$. 由 5.5.1(iii), z 是 A 上的整元. ∎

推论 5.5.6 设 C 是 A 在 R 中的整闭包. 则 C 在 R 中整闭.

证 设 C' 是 C 在 R 中的整闭包. 由5.5.5, C' 在 A 上是整的, 所以 $C'\subseteq C$, 从而 $C'=C$. ∎

下面我们将证明, 一个环在其子环上的整性可以推移到相应的剩余类环和分式环上去.

设 A 是环 R 的一个子环, $\mathfrak{r}$ 是 R 的一个理想. 令 $\mathfrak{a}=\mathfrak{r}\cap A$. 则 $\mathfrak{a}$ 显然是 A 的一个理想. 考虑自然同态 $R\longrightarrow R/\mathfrak{r}$. 在这个同态之下, 对于 $a\in A$,

$$A/\mathfrak{a}\in a+\mathfrak{a}\longmapsto a+\mathfrak{r}\in R/\mathfrak{r}$$

是同态单射, 因此可以把 $\{a+\mathfrak{r}\mid a\in A\}\subseteq R/\mathfrak{r}$ 与 $A/\mathfrak{a}$ 等同看待. 在这个意义下, 将 $A/\mathfrak{a}$ 看作 $R/\mathfrak{r}$ 的一个子环.

定理 5.5.7 设 R 是环 A 的一个整扩环.

(i) 设 $\mathfrak{r}$ 是 R 的一个理想, $\mathfrak{a}=\mathfrak{r}\cap A$. 则剩余类环 $R/\mathfrak{r}$ 是 $A/\mathfrak{a}$ 上的整扩环.

(ii) 设 S 是 A 的一个乘法闭子集. 则分式环 $S^{-1}R$ 是分式环 $S^{-1}A$ 上的整扩环.

证 (i) 设 $x\in R$. 我们有

$$x^n+a_1x^{n-1}+\cdots+a_n=0,\quad a_i\in A\ (1\leqslant i\leqslant n).$$

令 $\bar{x}=x+\mathfrak{r}$. 对于 $a\in A$, 令 $\bar{a}=a+\mathfrak{a}\in A/\mathfrak{a}$. 则

$$\bar{x}^n+\bar{a}_1\bar{x}^{n-1}+\cdots+\bar{a}_n=0,\quad \bar{a}_i\in A/\mathfrak{a}\ (1\leqslant i\leqslant n).$$

所以 $R/\mathfrak{r}$ 在 $A/\mathfrak{a}$ 上是整的.

(ii) $S^{-1}R$ 的任意元素可以表成 x/s 的形式, 这里 $x\in R$, $s\in S$. 由 x 所满足的方程得

$$(x/s)^n+(a_1/s)(x/s)^{n-1}+\cdots+a_n/s^n=0,$$

所以 x/s 是 $S^{-1}A$ 上的整元. ∎

定理 5.5.8 设 A 是环 R 的一个子环, C 是 A 在 R 中的整闭

包，S是A环的一个乘法闭子集．则$S^{-1}C$是$S^{-1}A$在$S^{-1}R$中的整闭包．

证 由5.5.7，$S^{-1}C$在$S^{-1}A$上是整的．设$r/s\in S^{-1}R$是$S^{-1}A$上一个整元．则有，

$$(r/s)^n+(a_1/s_1)(r/s)^{n-1}+\cdots+a_n/s_n=0$$

$a_i\in A$，$s_i\in S(1\leqslant i\leqslant n)$．令$t=s_1\cdots s_n\in S$．把上式两边同乘以$(st)^n$得

$$(rt)^n+a_1ss_2\cdots s_n(rs)^{n-1}+\cdots+a_ns_1\cdots s_{n-1}s^nt^n=0.$$

所以rt是A上的整元，从而$rt\in C$．所以$r/s=rt/st\in S^{-1}C$．

现在设A是一个整环．如果A在它的商域内是整闭的，那么就称A是一个**整闭整环**．

定理 5.5.9 唯一因子分解整环是整闭整环．

证 设A是一个唯一因子分解整环，K是A的商域．设$a/b\in K$，$a,b\in A$，$(a,b)=1$．如果a/b是A上整元，那么等式

$$a^n+a_1a^{n-1}b+\cdots+a_nb^n=0,\quad a_i\in A(1\leqslant i\leqslant n),$$

成立．所以

$$a^n=-a_1a^{n-1}b-\cdots-a_nb^n.$$

如果b是A的可逆元素，则$a/b\in A$．如果b不是A的可逆元素，则存在A的一个素元p，使得$p|b$，从而$p|a^n$．所以$p|a$，这与$(a,b)=1$的假设矛盾．这样，K在A上的整元都属于A，即A在K内是整闭的． ▌

推论 5.5.10 整数环$\mathbf{Z}$，一个域F上的n个不定元多项式环$F[X_1,\cdots,X_n]$都是整闭整环． ▌

习　题

1. 设B是环A的一个整扩环，$f: B\longrightarrow\bar{B}$是环同态，且$f(1_B)=1_{\bar{B}}$．则$f(B)$是$f(A)$的整扩环．

2. 设B是环A的整扩环．则$B[X_1,\cdots,X_n]$是$A[X_1,\cdots,$

X_n]的整扩环。

3. 设R是一个有单位元的交换环，$\{A_i\}$，$\{B_i\}$，$i\in I$，是R的子环族，且$A_i\subseteq B_i\subseteq R$，$\forall i\in I$。如果$A_i$在$B_i$中整闭，$\forall i\in I$，则$\bigcap_{i\in I} A_i$在$\bigcap_{i\in I} B_i$中整闭。

4. 设R是一个整环。证明下列断言是等价的：

（i） R是整闭的；

（ii） 对于每一个素理整$\mathfrak{p}$，$R_{\mathfrak{p}}$是整闭的；

（iii） 对于每一个极大理想$\mathfrak{m}$，$R_{\mathfrak{m}}$是整闭的。

5.6 整扩张与素理想

我们将讨论一个环与其整扩环的素理想之间的一些关系。先证明一个事实。

定理 5.6.1 设R是一个整环，A是R的一个子环，并且R在A上是整的，那么R是域必要且只要A是域。

证 设A是域。我们证明，R的每一个非零元素在R中有逆元。设$y\in R$，$y\neq 0$。因为y是A上的整元，所以存在A上一个次数大于零的多项式$f(X)$，使$f(y)=0$。设

$$f(X)=X^n+a_1X^{n-1}+\cdots+a_n\in A[X]$$

是以y为根的多项式中次最低的一个。我们有

$$y^n+a_1y^{n-1}+\cdots+a_n=0.$$

因为R是整环，所以$a_n\neq 0$。因此

$$y^{-1}=-a_n^{-1}(y^{n-1}+a_1y^{n-2}+\cdots+a_{n-1})\in R.$$

反之，设R是域。则A中任意非零元素x在R中有逆元x^{-1}。因为x^{-1}是A上的整元，所以有

$$(x^{-1})^m+a'_1(x^{-1})^{m-1}+\cdots+a'_m=0,\ a'_i\in A(1\leqslant i\leqslant m).$$

两边乘以x^{m-1}，我们得到

$$x^{-1}=-(a'_1+a'_2x+\cdots+a'_mx^{m-1})\in A. \quad ■$$

推论 5.6.2 设R是环A上一个整扩环，$\mathfrak{q}$是R的一个素理

想。令 $\mathfrak{p}=\mathfrak{q}\cap A$。那么 $\mathfrak{q}$ 是 R 的极大理想必要且只要 $\mathfrak{p}$ 是 A 的极大理想。

证 $R/\mathfrak{q}$ 是整环。由5.5.7，$R/\mathfrak{q}$ 是 $A/\mathfrak{p}$ 上的整扩环。于是由5.6.1，$\mathfrak{q}$ 是 R 的极大理想 $\Longleftrightarrow R/\mathfrak{q}$ 是域 $\Longleftrightarrow A/\mathfrak{p}$ 是域 $\Longleftrightarrow \mathfrak{p}$ 是 A 的极大理想。 ▮

推论 5.6.3 设 R 是环 A 上一个整扩环，$\mathfrak{q}_1$ 和 $\mathfrak{q}_2$ 都是 R 的素想理，且 $\mathfrak{q}_1\subseteq\mathfrak{q}_2$。如果 $\mathfrak{q}_1\cap A=\mathfrak{q}_2\cap A$，则 $\mathfrak{q}_1=\mathfrak{q}_2$。

证 令 $\mathfrak{p}=\mathfrak{q}_1\cap A=\mathfrak{q}_2\cap A$。则 $\mathfrak{p}$ 是 A 的素理想。由5.5.7，R 对 $\mathfrak{p}$ 的分式环 $R_{\mathfrak{p}}$ 是 A 对 $\mathfrak{p}$ 的分式环 $A_{\mathfrak{p}}$ 上的整扩环。令 $\mathfrak{m}=\mathfrak{p}A_{\mathfrak{p}}$，$\mathfrak{n}_1=\mathfrak{q}_1R_{\mathfrak{p}}$，$\mathfrak{n}_2=\mathfrak{q}_2R_{\mathfrak{p}}$。则 $\mathfrak{m}$ 是 $A_{\mathfrak{p}}$ 的唯一的极大理想。我们有

$$\mathfrak{n}_1\cap A_{\mathfrak{p}}=\mathfrak{n}_2\cap A_{\mathfrak{p}}=\mathfrak{m}.$$

由5.6.2，$\mathfrak{n}_1$ 和 $\mathfrak{n}_2$ 都是 R 的极大理解。但 $\mathfrak{n}_1\subseteq\mathfrak{n}_2$，所以 $\mathfrak{n}_1=\mathfrak{n}_2$。因此，$\mathfrak{q}_1=\mathfrak{n}_1\cap R=\mathfrak{n}_2\cap R=\mathfrak{q}_2$。 ▮

定理 5.6.4 （位于上(Lying over)定理）设 R 是环 A 的一个整扩环，$\mathfrak{p}$ 是 A 的一个素理想。那么存在 R 的一个素理想 $\mathfrak{q}$，使得 $\mathfrak{q}\cap A=\mathfrak{p}$。

证 由5.5.7，分式环 $R_{\mathfrak{p}}$ 是分式环 $A_{\mathfrak{p}}$ 的整扩环。下面的图显然是交换的：

$$\begin{array}{ccc} A & \xrightarrow{\psi_A} & A_{\mathfrak{p}} \\ \downarrow & & \downarrow \\ R & \xrightarrow[\psi_R]{} & R_{\mathfrak{p}} \end{array}$$

在这个图里，垂直的箭头表示自然内射，$\psi_A: A\longrightarrow A_{\mathfrak{p}}$，$\psi_R: R\longrightarrow R_{\mathfrak{p}}$ 是自然同态。$\psi_R|_A=\psi_A$。

令 $\mathfrak{n}$ 是 $R_{\mathfrak{p}}$ 的一个极大理想，$\mathfrak{m}=\mathfrak{n}\cap A_{\mathfrak{p}}$。由5.6.2，$\mathfrak{m}$ 是 $A_{\mathfrak{p}}$ 的极大理想。然而 $A_{\mathfrak{p}}$ 是局部环，它有唯一的极大理想

$\mathfrak{p}A_{\mathfrak{p}}$。所以 $\mathfrak{m}=\mathfrak{p}A_{\mathfrak{p}}$。$\mathfrak{q}=\psi_R^{-1}(\mathfrak{m})$是$R$的一个素理想，而 $\mathfrak{q}\cap A=\psi_A^{-1}(\mathfrak{n}\cap A_{\mathfrak{p}})=\psi_A^{-1}(\mathfrak{n})=\mathfrak{p}A_{\mathfrak{p}}\cap A=\mathfrak{p}$。 ∎

定理 5.6.5（上升(Going up)定理）设R是环A上一个整扩环. $\mathfrak{p}_1\subseteq\mathfrak{p}_2\subseteq\cdots\subseteq\mathfrak{p}_n$ 是 A 的一个素理想链，$\mathfrak{q}_1\subseteq\cdots\subseteq\mathfrak{q}_m(m<n)$是$R$的一个素理想链，且$\mathfrak{q}_i\cap A=\mathfrak{p}_i(1\leqslant i\leqslant m)$。那么存在$R$的一个素理想链，$\mathfrak{q}_1\subseteq\cdots\subseteq\mathfrak{q}_m\subseteq\mathfrak{q}_{m+1}\subseteq\cdots\subseteq\mathfrak{q}_n$，使得$\mathfrak{q}_i\cap A=\mathfrak{p}_i(1\leqslant i\leqslant n)$。

证 对m,n作双重数学归纳法。只需对$m=1$，$n=2$的情形证明即可。

设 $\mathfrak{p}_1\subseteq\mathfrak{p}_2$，$\mathfrak{p}_1,\mathfrak{p}_2$都是$A$的素理想，$\mathfrak{q}_1$是$R$的素理想且$\mathfrak{q}_1\cap A=\mathfrak{p}_1$。令$\bar{A}=A/\mathfrak{p}_1$，$\bar{R}=R/\mathfrak{q}_1$。由5.5.7，$\bar{R}$是$\bar{A}$的整扩环。令$\bar{\mathfrak{p}}_2$是在自然同态$A\longrightarrow\bar{A}$之下，$\mathfrak{p}_2$的象，则$\bar{\mathfrak{p}}_2$是$\bar{A}$的素理想。由5.6.4，存在$\bar{R}$的素理想$\bar{\mathfrak{q}}_2$，使得$\bar{\mathfrak{q}}_2\cap\bar{A}=\bar{\mathfrak{p}}_2$。令$\psi: R\longrightarrow R/\mathfrak{q}_1$是自然同态。令$\mathfrak{q}_2=\psi^{-1}(\bar{\mathfrak{q}}_2)$。则$\mathfrak{q}_2$是$R$的素理想。我们有$\mathfrak{q}_1\subseteq\mathfrak{q}_2$，$\mathfrak{q}_2\cap A=\mathfrak{p}_2$。 ∎

习 题

1. 设R是环A的一个整扩环，$\mathfrak{q}$是R中位于A的素理想$\mathfrak{p}$之上的一个素理想(即$\mathfrak{q}\cap A=\mathfrak{p}$)。证明，$\mathfrak{q}$是$R$的极大理想必要且只要$\mathfrak{p}$是$A$的极大理想。

2. 设A是环R的一个子环。

(i) 如果$\mathfrak{a}\neq R$是R的一个理想，则$\mathfrak{a}\cap A\neq A$且$\mathfrak{a}\cap A$是A的一个理想。

(ii) 如果$\mathfrak{q}$是R的一个素理想，则$\mathfrak{q}\cap A$是A的一个素理思。

3. 设C是环A在扩环B内的整闭包，$\mathfrak{a}$是A的一个理想，令$\mathfrak{a}C=\{\sum a_ic_i$（有限和）$|a_i\in\mathfrak{a}，c_i\in C\}$，则$\mathfrak{a}C$是$C$的一个理想。$B$的元素$x$说是在$\mathfrak{a}$上整的，如果$x$满足一个形如

$$x^n + a_1x^{n-1} + \cdots + a_n = 0$$

的方程，$a_i \in \mathfrak{a}\ (1 \leqslant i \leqslant n)$。证明$B$的所有在 $\mathfrak{a}$ 上整元素所成的集等于$\sqrt{\mathfrak{a}C}$。

4. 设$A \subseteq B$是整环，其中A是整闭的，F是A的商域。又设$\alpha \in B$是A的一个理想$\mathfrak{a}$上的整元素。证明，α是F上的代数元。令$f(X) = X^n + a_1X^{n-1} + \cdots + a_n$是$\alpha$在$F$上的最小多项式，则$a_1, \cdots, a_n \in \sqrt{\mathfrak{a}}$。

5. （下降（Going down）定理）令$A \subseteq B$是整环，其中A是整闭的，而B在A上是整的。令$\mathfrak{p}_1 \supseteq \cdots \supseteq \mathfrak{p}_n$是$A$的一个素理想链，$\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m (m < n)$是$B$的素理想链，使得$\mathfrak{q}_i \cap A = \mathfrak{p}_i (1 \leqslant i \leqslant m)$。那么链 $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_m$ 可以延长到素理想链 $\mathfrak{q}_1 \supseteq \cdots \supseteq \mathfrak{q}_n$，使得$\mathfrak{q}_i \cap A = \mathfrak{p}_i\ (1 \leqslant i \leqslant n)$。

5.7 Noether的正规化定理

定理 5.7.1 （Noether 的正规化定理）设F是一个域，R是F上有限个元素$x_1, \cdots, x_n$生成的环，那么存在$y_1, \cdots, y_m \in R$ $(m \leqslant n)$，使得以下两个条件被满足：

（ i ） $y_1, \cdots, y_m$在F上代数无关；

（ ii ） R在子整环$F[y_1, \cdots, y_m]$上是整的。

证 对n作数学归纳法。$n = 1$时，$R = F[x_1]$。如果x_1是F上的超越元，那么就取 $y_1 = x_1$；如果 x_1 在F上是代数元，这时$m = 0$。

设$n > 1$，如果$x_1, \cdots, x_n$在F上代数无关，则 $m = n$，$y_i = x_i$ $(1 \leqslant i \leqslant m = n)$。定理已成立。现在设 $x_1, \cdots, x_n$ 在F上代数相关。于是存在F上n个不定元$X_1, \cdots, X_n$的多项式

$$f(X_1, \cdots, X_n) = \sum_{(i) = (i_1, \cdots, i_n)} a_{(i)} x_1^{i_1} \cdots x_n^{i_n} \neq 0,$$

使得$f(x_1, \cdots, x_n) = 0$。

取定一个正整数 t，使得 t 大于出现在 f 里的一切指数组 $(i)=(i_1,\cdots,i_n)$ 的每一个分量。由整数的带余除法，每一个整数 s 可以唯一地表成 t 进整数

$$s=r_1+r_2t+\cdots+r_kt^{k-1},\quad 0\leqslant r_i<t.$$

现在令

$$z_i=x_i-x_1^{t^{i-1}},\quad x_i=z_i+x_1^{t^{i-1}}\ (2\leqslant i\leqslant n)$$

代入 $f(x_1,\cdots,x_n)=0$ 中，我们有

$$\sum_{(i)}a_{(i)}x_1^{i_1}(z_2+x_1^t)^{i_2}\cdots(z_n+x_1^{t^{n-1}})^{i_n}=0.$$

整理以后，上式可以写成

$$(*)\qquad \sum_{(i)}a_{(t)}x_1^{i_1+i_2t+\cdots+i_nt^{n-1}}+g(x_1,z_2,\cdots,z_n)=0,$$

这里 $g(x_1,z_2,\cdots,z_n)$ 是一个多项式，它的每一项至少含有某一个 z_i。

根据 t 的取法，如果 $(i)=(i_1,\cdots,i_n)\neq(j)=(j_1,\cdots,j_n)$ 是 f 中两个不同的指数组，则

$$i_1+i_2t+\cdots+i_nt^{n-1}\neq j_1+j_2t+\cdots+j_nt^{n-1}.$$

因此，在对应于 f 的指数组 $(i)=(i_1,\cdots,i_n)$ 的正整数 $i_1+i_2t+\cdots+i_nt^{n-1}$ 中，有唯一的最大数 s。设 $s=p_1+p_2t+\cdots+p_nt^{n-1}$ 对应于指数组 $(p)=(p_1,\cdots,p_n)$。于是 $(*)$ 可以写成

$$ax_1^s+\sum_{j<s}u_j(z_2,\cdots,z_n)x_1^j=0,$$

这里 $a=a_{(p)}\neq 0$，$u_j(z_2,\cdots,z_n)\in F[z_2,\cdots,z_n]$。两边乘以 a^{-1} 得

$$x_1^s+\sum_{j<s}a^{-1}u_j(z_2,\cdots,z_n)x^j=0.$$

所以 x_1 是 $F[z_2,\cdots,z_n]$ 上的整元。又 $x_i=z_i+x_1^{t^{i-1}}$ $(2\leqslant i\leqslant n)$，

所以 $x_i(2\leqslant i\leqslant n)$ 也是 $F[z_2,\cdots,z_n]$ 上的整元。这样，$R=F[x_1,$

$\cdots, x_n]$ 是环 $F[z_2, \cdots, z_n]$上的整扩环。

由归纳法的假设，存在 $y_1, \cdots, y_m \in F[z_2, \cdots, z_n]$，$m \leqslant n-1$，使得$y_1, \cdots, y_m$在$F$上代数无关，并且$F[z_2, \cdots, z_n]$在$F[y_1, \cdots, y_m]$上是整的。于是由5.5.5，$R = F[x_1, \cdots, x_n]$在$F[y_1, \cdots, y_m]$上是整的。定理被证明。 ▮

如果域F含有无限多个元素，那么定理 5.7.1 还可以进一步精确化。

定理 5.7.2 设F是一个无限域，$R = F[x_1, \cdots, x_n]$ 是一个整环。那么存在 $y_1, \cdots, y_m \in R\ (m \leqslant n)$，使得下列条件被满足：

（ i ） $y_1, \cdots, y_m$ 在F上代数无关；

（ ii ） R在子整环 $F[y_1, \cdots, y_m]$ 上是整的；

（iii） 每一个y_i可以表成 $y_i = \sum_{j=1}^{n} c_{ij} x_j\ (c_{ij} \in F)$ 的形式，

$1 \leqslant i \leqslant m$。

证 对n作数学归纳法。$n=1$时定理成立。设$n>1$。如果$x_1, \cdots, x_n$ 在F上代数无关，则取 $y_i = x_i\ (1 \leqslant i \leqslant m = n)$，这时定理自然成立。设$x_1, \cdots, x_n$在$F$上代数相关。于是存在 $F[X_1, \cdots, X_n]$ 的非零多项式

$$f(X_1, \cdots, X_n) = \sum_{(i)} a_{(i)} X_1^{i_1} \cdots X_n^{i_n} \neq 0,$$

使得 $f(x_1, \cdots, x_n) = 0$。取 $c_2, \cdots, c_n \in F$。令

$$z_i = x_i - c_i x_1,\quad x_i = z_i + c_i x_1,\quad 2 \leqslant i \leqslant n,$$

这里 $c_2, \cdots, c_m \in F$ 以后再确定。代入 $f(x_1, \cdots, x_n) = 0$，得

$$\sum_{(i)} a_{(i)} x_1^{i_1} (z_2 + c_2 x_1)^{i_2} \cdots (z_n + c_n x_1)^{i_n} = 0.$$

整理以后得

$$\sum_{(i)} a_{(i)} c_2^{i_2} \cdots c_n^{i_n} x_1^{i_1 + i_2 + \cdots + i_n} + g(x_1, z_2, \cdots, z_n) = 0,$$

这里 $g(x_1,z_2,\cdots,z_n)\in F[x_1,z_2,\cdots,z_n]$，并且每一项至少含有某一个 z_i。

上面的等式左边第一项是 x_1 的多项式。设其次数为 s，$s=\max\limits_{(i)}(i_1+i_2+\cdots+i_n)$。注意到 $g(x_1,z_2,\cdots,z_n)$ 中，x_1 的次数都小于 s，所以上式可以写成

$$a(c_2,\cdots,c_n)x_1^s+\sum_{j<s}u_j(z_2,\cdots,z_n)x_1^j=0,$$

这里 $a(Y_2,\cdots,Y_n)$ 是 F 上 n-1 个不定元 $Y_2,\cdots,Y_n$ 的一个多项式：

$$(2)\qquad a(Y_2,\cdots,Y_n)=\sum_{k_1+k_2+\cdots+k_n=s}b_{k_1,\cdots,k_n}Y_2^{k_2}\cdots Y_n^{k_n}.$$

因为F是无限域，所以总存在$c_2,\cdots,c_n\in F$，使得$a(c_2,\cdots,c_n)\neq 0$。取定一组 $c_2,\cdots,c_n\in F$，使得 $c=a(c_2,\cdots,c_n)\neq 0$。以 c^{-1} 乘(2)式的两端得

$$x_1^s+\sum_{j<s}c^{-1}u_j(z_2,\cdots,z_n)x_1^j=0.$$

所以 x_1 是$F[z_2,\cdots,z_n]$上的整元，从而 $x_i=z_i+c_ix_1(2\leqslant i\leqslant n)$ 也是$F[z_2,\cdots,z_n]$上的整元。因此，$R=F[x_1,\cdots,x_n]$ 在$F[z_2,\cdots,z_n]$上是整的。

由归纳法的假设，存在 $y_1,\cdots,y_m(m\leqslant n-1)\in F[z_2,\cdots,z_n]$，使得 (i) $y_1,\cdots,y_m$ 在 F 上代数无关；(ii) $F[z_2,\cdots,z_n]$ 在$F[y_1,\cdots,y_m]$ 上是整的；(iii) $y_i=\sum\limits_{j=2}^{n}d_{ij}z_j\,(d_{ij}\in F,\ 1\leqslant i\leqslant m)$。由5.5.5，$R$在$F[y_1,\cdots,y_m]$上是整的。由于$z_j=x_j-c_jx_1(2\leqslant j\leqslant n)$，所以

$$y_i=\sum_{j=1}^{n}c_{ij}x_j,\quad c_{ij}\in F\,(1\leqslant i\leqslant m).$$

定理被证明。 ▮

5.8 代数簇 Hilbert 零点定理

从历史上来看，求一组多项式的公共零点问题是代数学的中心问题．这个问题尚远远未能解决．在高等代数里曾经讨论了这个问题的两个最简单的情形，就是某一个数域上 n 元一次多项式组（线性方程组）和一元 n 次多项式的情形．在这一节里，我们将一般地讨论一组多项式的公共零点的存在问题．

设K是一个域．为了简单起见，在这一节里，我们总假定K是代数闭域．令

$$K^n=\{(x_1,\cdots,x_n)\mid x_i\in K\}$$

是K上n维向量空间，称为K上n维仿射空间．K^n中的元素叫做点．令$K[X_1,\cdots,X_n]$是K上n个不定元的多项式环．为了简单起见，我们把$K[X_1,\cdots,X_n]$简记作$K[X]$，把$f(X_1,\cdots,X_n)$简记作$f(X)$，把K^n中的向量$(x_1,\cdots,x_n)$简记作(x)，把$f(X)$在$(x)=(x_1,\cdots,x_n)$的值$f(x_1,\cdots,x_n)$简记作$f(x)$。

设S是$K[X]$的一个子集．令

$$V(S)=\{(x)\in K^n\mid f(x)=0,\ \forall f\in S\}.$$

$V(S)$叫做K^n中一个**仿射代数簇**，或简称为**代数簇**．

令$\mathfrak{a}$是S在$K[x]$内所生成的理想．那么显然有

$$V(S)=V(\mathfrak{a}).$$

设M是K^n的一个子集．令

$$I(M)=\{f\in K[X]\mid f(x)=0,\ \forall(x)\in M\}.$$

那么$I(M)$是$K[X]$的一个理想．

关于运算V和I，以下性质成立．

定理 5.8.1 运算V和运算I有下列性质：

（i） $I(K^n)=(0)$；$I(\varnothing)=(1)=K[X]$.

（ii） 对于K^n的每一个子集M来说，

$$I(M)=\sqrt{I(M)}.$$

(iii) 对于每一个代数簇$A\subseteq K^n$，我们有

$$V(I(A))=A.$$

(iv) 设A_1, A_2是K上两个代数簇.

$$A_1\subseteq A_2 \Longleftrightarrow I(A_1)\supseteq I(A_2),$$

并且$A_1\subsetneqq A_2 \Longleftrightarrow I(A_1)\supsetneqq I(A_2)$.

(v) 设M_1, M_2是K^n的两个子集，则

$$I(M_1\cup M_2)=I(M_1)\cap I(M_2).$$

(vi) 设$\mathfrak{a}$，$\mathfrak{b}$是$K[X]$的两个理想. 则

$$V(\mathfrak{a}\ \mathfrak{b})=V(\mathfrak{a}\cap\mathfrak{b})=V(\mathfrak{a})\cup V(\mathfrak{b}).$$

(vii) 设$\{\mathfrak{a}_\lambda\}_{\lambda\in\Lambda}$是$K[X]$的一族理想. 令

$$\sum_\lambda \mathfrak{a}_\lambda=\{\sum_\lambda f_\lambda\ (\text{有限和})\mid f_\lambda\in\mathfrak{a}_\lambda, \lambda\in\Lambda\}$$

是$\{\mathfrak{a}_\lambda\}_{\lambda\in V}$所生成的理想. 则

$$V(\sum\mathfrak{a}_\lambda)=\bigcap_\lambda V(\mathfrak{a}_\lambda).$$

(viii) 设$\{M_\lambda\}_{\lambda\in\Lambda}$是$K^n$的一族子集. 则

$$I(\bigcup_\lambda M_\lambda)=\bigcap_\lambda I(M_\lambda).$$

证 (i) 显然$I(\varnothing)=(1)=K[X]$. 因为K是代数闭域，所以是无限域. 这样就有$I(K^n)=(0)$.

(ii) 只需证$\sqrt{I(M)}\subseteq I(M)$. 设$f\in\sqrt{I(M)}$，则存在正整数$m$，使得$f^m\in I(M)$. 于是$f(x)^m=0$，$\forall(x)\in M$，从而$f(x)=0$，$\forall(x)\in M$. 所以$f\in I(M)$.

(iii) 显然$A\subseteq V(I(A))$，反之，设A是$K[X]$的某一个子集S的公共零点的集. 则$S\subseteq I(A)$. 于是$A=V(S)\supseteq V(I(A))$.

(iv) 若$A_1\subseteq A_2$，那么显然$I(A_1)\supseteq I(A_2)$. 反之，若$I(A_1)\supseteq I(A_2)$，那么由(iii) $A_1=V(I(A_1))\subseteq V(I(A_2))=A_2$. 由此很容易得出第二个论断.

(v) $M_i\subseteq M_1\cup M_2$，所以$I(M_1\cup M_2)\subseteq I(M_i)$，$i=1,2$. 从而$I(M_1\cup M_2)\subseteq I(M_1)\cap I(M_2)$. 反之，设$f\notin I(M_1\cup M_2)$.

那么存在$(x)\in M_1\cup M_2$，使得$f(x)\neq 0$．于是$f\notin I(M_1)$或$f\notin I(M_2)$，从而$f\notin I(M_1)\cap I(M_2)$．

(vi) 因为$\mathfrak{a}\mathfrak{b}\subseteq\mathfrak{a}\cap\mathfrak{b}\subseteq\mathfrak{a},\mathfrak{b}$．所以

$$V(\mathfrak{a}\mathfrak{b})\supseteq V(\mathfrak{a}\cap\mathfrak{b})\supseteq V(\mathfrak{a})\cup V(\mathfrak{b}).$$

反之，设$(x)\notin V(\mathfrak{a})\cup V(\mathfrak{b})$．则$(x)\notin V(\mathfrak{a})$且$(x)\notin V(\mathfrak{b})$．于是存在$f\in\mathfrak{a}$，$g\in\mathfrak{b}$，使得$f(x)\neq 0$，$g(x)\neq 0$，从而$fg(x)\neq 0$．然而$fg\in\mathfrak{a}\mathfrak{b}$．所以$(x)\notin V(\mathfrak{a}\mathfrak{b})$．

(vii) $\sum_{\lambda}\mathfrak{a}_{\lambda}\supseteq\mathfrak{a}_{\lambda}$，$\forall\lambda\in\Lambda$．所以$V(\sum_{\lambda}\mathfrak{a}_{\lambda})\subseteq\bigcap_{\lambda}V(\mathfrak{a}_{\lambda})$．反之，设$(x)\notin V(\sum_{\lambda}\mathfrak{a}_{\lambda})$，那么存在$f\in\sum_{\lambda}\mathfrak{a}_{\lambda}$，使得$f(x)\neq 0$．设$f=\sum^{s}f_i$，$f_i\in\mathfrak{a}_{\lambda_i}$，$\lambda_i\in\Lambda$．那么至少有一个$f_i(x)\neq 0$．从而$(x)\notin\mathfrak{a}_{\lambda_i}$，对某一$\lambda_i\in\Lambda$．所以$(x)\notin\bigcap_{\lambda}V(\mathfrak{a}_{\lambda})$．

(viii) 与(vii)的证明类似． ∎

设$\mathfrak{a}$是$K[X]$的一个理想．如果$\mathfrak{a}=\sqrt{\mathfrak{a}}$，那么就称$\mathfrak{a}$是一个**根理想**．

令$\mathfrak{A}$是K^n中一切代数簇所成的集，令$\mathfrak{R}$是$K[X]$中一切根理想所成的集．由5.8.1(ii)和(iv)，映射$I: \mathfrak{A}\in A\longrightarrow I(A)\in\mathfrak{R}$是一个单射，并且反向保持包含关系．即$A_1\subseteq A_2\Longrightarrow I(A_1)\supseteq(A_2)$．下面我们将会看到，这个映射也是满射．

K^n中一个代数簇A说是**不可约的**，如果以下条件被满足：若$A=A_1\cup A_2$，其中A_1，A_2都是代数簇，那么或者$A=A_1$，或者$A=A_2$．

定理 5.8.2 K^n中一个代数簇A是不可约的，必要且只要$I(A)$是$K[X]$的素理想．

证 设A不可约，$f_1,f_2\in K[X]$且$f_1f_2\in I(A)$．令

$$V(f_i)=\{(x)\in K^n\,|\,f_i(x)=0\},\ i=1,2.$$

令$A_i=A\cap V(f_i)$，$i=1,2$．则由5.8.1 (vii)，A_1，A_2都是代数

簇。因为$f_1f_2(x)=0$，$\forall(x)\in A$，所以$f_1(x)=0$或$f_2(x)=0$。因此 $A\subseteq V(f_1)\cup V(f_2)$，从而 $A=A_1\cup A_2$。于是有$A=A_1$或$A=A_2$。由此得出 $A\subseteq V(f_1)$ 或 $A\subseteq V(f_2)$。因此 $f_1\in I(A)$或$f_2\in I(A)$。所以$I(A)$是素理想。

反之，设 $I(A)$ 是素理想。假设存在代数簇A_1，A_2，使得$A=A_1\cup A_2$，且 $A_2\subsetneq A$. 则由5.8.1（iv）和（v），我们有$I(A)\subsetneq I(A_2)$ 且 $I(A)=I(A_1)\cap I(A_2)=I(A_1)\ I(A_2)$。于是由5.3.1（ii），我们有$I(A_1)\subseteq I(A)$，从而 $A_1=A$。所以A是不可约的。 ∎

设 $A_i\subseteq K^n$ 是代数簇，$i=1,2,\cdots$，并且

$$A_1\supseteq A_2\supseteq\cdots\supseteq A_n\supseteq\cdots.$$

与此相应，有 $K[x]$ 中一个理想升链

$$I(A_1)\subseteq I(A_2)\subseteq\cdots\subseteq I(A_n)\subseteq\cdots.$$

因为$K[x]$是 Noether 环，所以存在一个正整数n，使得$I(A_n)=I(A_{n+1})=\cdots$。于是由5.8.1（iv），我们有 $A_n=A_{n+1}=\cdots$。这时我们说，代数簇满足降链条件。

定理 5.8.3 K^n中每一个代数簇都可以表成有限个不可约代数簇的并。

证 设 A 是一个代数簇. 如果 A 不可约，那么论断自然成立。否则 $A=A_1\cup A'_1$，其中A_1，A'_1都是代数簇，且$A_1\subsetneq A$，$A'_1\subsetneq A$，如果 A_1与A'_1中至少有一个不能表成有限个不可约代数簇的并，比方说，A_1 不能表成有限个不可约代数簇的并，那么对 A_1 作同样的讨论，就存在一个代数簇 $A_2\subsetneq A_1$，并且 A_2不能表成有限个不可约代数簇的并. 如此继续下去。于是就得到代数簇的一个无限降链

$$A\supsetneq A_1\supsetneq A_2\supsetneq\cdots.$$

这就导致矛盾。 ∎

定理 5.8.4 设A是一个代数簇. 如果

$$A = A_1 \cup \cdots \cup A_r = A'_1 \cup \cdots \cup A'_s,$$

其中A_i, A'_j都是不可约代数簇，并且$A_i \not\subseteq A_k$, $A'_j \not\subseteq A'_l$若 $i \neq k$, $j \neq l$。那么$r = s$，并且可以适当排列A'_j的次序，使得$A_i = A'_i$，$1 \leqslant i \leqslant r = s$。

证 首先注意以下事实，设A是一个不可约代数簇。如果

$$A \subseteq A_1 \cup \cdots \cup A_s,$$

其中A_i是不可约代数簇($1 \leqslant i \leqslant s$)，那么必有某一个$j$($1 \leqslant j \leqslant s$)，使得$A \subseteq A_j$。

事实上，我们有$A = \bigcup_{i=1}^{s}(A \cup A_i)$。因为$A$不可约，所以存在一个$j$($1 \leqslant j \leqslant s$)，使得$A = A \cup A_j$。从而$A \subseteq A_j$。

现在设$A_1 \cup \cdots \cup A_r = A'_1 \cup \cdots \cup A'_s$，$A_i$, A'_j都是不可约代数簇($1 \leqslant i \leqslant r, 1 \leqslant j \leqslant s$)。则

$$A_1 \subseteq A'_1 \cup \cdots \cup A'_s.$$

于是由上面所证的事实，可设$A_1 \subseteq A'_1$。又因为

$$A'_1 \subseteq A_1 \cup \cdots \cup A_r,$$

所以存在某一个i，使得$A'_1 \subseteq A_i$。根据题设的条件，必须$i = 1$，从而$A_1 = A'_1$。这样，对r作数学归纳法，就证明了这个定理。 ∎

现在我们证明 Hilbert 零点定理，它是多项式组的零点存在定理。

定理 5.8.5 (零点定理) 设K是一个代数闭域，$K[X]$是K上n个不定元的多项式环，$\mathfrak{a}$是$K[X]$的一个理想。如果$\mathfrak{a} \neq K[X]$，则$V(\mathfrak{a}) \neq \varnothing$。

证 因为$\mathfrak{a} \neq K[X]$，所以存在$K[X]$的一个极大理想$\mathfrak{m} \supseteq \mathfrak{a}$。于是$B = K[X]/\mathfrak{m}$是一个域。令$x_i$是$X_i$所在的剩余类($1 \leqslant i \leqslant n$)。于是由 5.2.9，$B$是$K$上的代数扩域。因为$K$是代数闭域，所以$B = K$。于是$(x_1, \cdots, x_n) \in K^n$是$\mathfrak{m}$中多项式的一个公共零点，因而$(x_1, \cdots, x_n) \in V(\mathfrak{m}) \subseteq V(\mathfrak{a})$。 ∎

由这个定理，可以得出以下推论。

推论 5.8.6 设K是一个代数闭域．K上一个代数方程组

$$f_i(X_1,\cdots,X_n)=0,\ f_i\in K[X](1\leqslant i\leqslant m),$$

在K^n中有解必要且只要$(f_1,\cdots,f_n)\neq K[X]$.

证 令 $\mathfrak{a}=(f_1,\cdots,f_m)$。如果 $\mathfrak{a}\neq K[x]$，则由零点定理有 $V(\mathfrak{a})\neq\varnothing$，即方程组 $f_i=0\ (1\leqslant i\leqslant m)$ 在K^n中有解。如果 $\mathfrak{a}=K[X]=(1)$，那么显然 $V(\mathfrak{a})=\varnothing$。 ∎

推论 5.8.7 设K是一个代数闭域，$\mathfrak{m}$ 是$K[X]$的一个极大理想．那么存在 $a_1,\cdots,a_n\in K$，使得

$$\mathfrak{m}=(X_1-a_1,\cdots,X_n-a_n).$$

证 由零点定理，存在$(a)=(a_1,\cdots,a_n)\in V(\mathfrak{m})$。如果$f\in\mathfrak{m}$，那么$f(a_1,\cdots,a_n)\neq0$，因为不然的话，$(a)$将是$K[X]$的所有多项式的公共零点．因此$(X_1-a_1,\cdots,X_n-a_n)\subseteq\mathfrak{m}$.然而$(X_1-a_1,\cdots,X_n-a_n)$本身已是一个极大理想，所以

$$\mathfrak{m}=(X_1-a_1,\cdots,X_n-a_n).$$ ∎

定理 5.8.8 设K是一个代数闭域，$\mathfrak{a}$是$K[X]$的一个理想．则

$$\sqrt{\mathfrak{a}}=I(V(\mathfrak{a})).$$

证 对于$K[X]$的任意理想$\mathfrak{a}$来说都有$\sqrt{\mathfrak{a}}\subseteq I(V(\mathfrak{a}))$。现在设$f\in I(V(\mathfrak{a}))$。我们借助于所谓"Rabinovich 的巧思"来证明 $f\in\sqrt{\mathfrak{a}}$.

在$K[X_1,\cdots,X_n]$上添加一个新的不相关不定元T．在多项式环$K[X_1,\cdots,X_n,T]$中考虑由$\mathfrak{a}$及$fT-1$所生成的理想$\mathfrak{b}$．如果$(x_1,\cdots,x_n,t)\in K^{n+1}$是$\mathfrak{b}$中多项式的一个公共零点，那么将有$(x_1,\cdots,x_n)\in V(\mathfrak{a})$，从而$f(x_1,\cdots,x_n)t-1=-1$.然而$(x_1,\cdots,x_n,t)$是$f\cdot T-1$的零点，这就导致矛盾.因此$\mathfrak{b}$在$K^{n+1}$中没有零点．由 5.8.5，$\mathfrak{b}=K[X_1,\cdots,X_n,T]$.

因为$K[X_1,\cdots,X_n]$是Noether环，所以$\mathfrak{a}$是由有限个元

素 $f_1,\cdots,f_s\in K[X_1,\cdots,X_n]$ 生成的。于是我们有

$$\sum_{i=1}^{s} f_i g_i + h(fT-1)=1,$$

这里 $g_i,\ h\in K[X_1,\cdots,X_n,T]$，$1\leqslant i\leqslant s$。

定义一个K-同态

$$\varphi: K[X_1,\cdots,X_n,T]\longrightarrow K(X_1,\cdots,X_n),$$

$$\varphi(X_i)=X_i(1\leqslant i\leqslant n),\ \varphi(T)=\frac{1}{f}.$$

于是在 $K(X_1,\cdots,X_n)$里，有

$$\sum_{i=1}^{s} f_i\varphi(g_i)=1,$$

这里

$$\varphi(g_i(X_1,\cdots,X_n,T))=g_i(X_1,\cdots,X_n,\frac{1}{f})=\frac{u_i}{f^{k_i}},$$

$u_i\in K[X_1,\cdots,X_n]$，k_i是一个非负整数。令 $k=\max\limits_{1\leqslant i\leqslant s}\{k_i\}$。

则 $f^k\in(f_1,\cdots,f_s)=\mathfrak{a}$，从而 $f\in\sqrt{\mathfrak{a}}$。 ∎

推论 5.8.9 设K是一个代数闭域，$\mathfrak{A}$是 K^n 中一切代数簇所成的集，$\mathfrak{R}$是$K[X]$中一切根理想所成的集。$I:\mathfrak{A}\in V\longrightarrow I(A)\in\mathfrak{R}$是一个双射。 ∎

推论 5.8.10 (i)设 $\mathfrak{a}$，$\mathfrak{b}$ 是 $K[X]$的两个理想，$V(\mathfrak{a})=V(\mathfrak{b})\Longleftrightarrow\sqrt{\mathfrak{a}}=\sqrt{\mathfrak{b}}$。

(ii) K上两个n元代数方程组

$$f_i(X_1,\cdots,X_n)=0\quad(i=1,\cdots,s),$$

和

$$g_j(X_1,\cdots,X_n)=0\quad(j=1,\cdots,t)$$

有相同的解必要且只要对于每一个 $i,1\leqslant i\leqslant s$，都有一个正整数 k_i，使得 $f_i^{k_i}\in(g_1,\cdots,g_t)$，同时对于每一个$j$，$1\leqslant j\leqslant t$，都有一个正整数 l_j，使得 $g_j^{l_j}\in(f_1,\cdots,f_s)$。

证 (i)是 5.8.1 (ii)和 5.8.9 的直接结果。在(i)中令 $\mathfrak{a}=(f_1,\cdots,f_s)$，$\mathfrak{b}=(g_1,\cdots,g_t)$，就得到(ii)。 ∎

习　题

设K是一个代数闭域，$K[X]=K[X_1,\cdots,X_n]$是K上n个不定元的多项式环。

1. 试举一例说明，存在$K[X]$的理想$\mathfrak{a}$，使得

$$I(V(\mathfrak{a}))\supsetneqq\mathfrak{a}。$$

2. $K[X]$中一个多项式f在K^n中的一切零点所成的集$V(f)$叫做一个超曲面。证明

（i） 对于每一个超曲面$V(f)$来说，一定存在K^n中无限个点不属于$V(f)$。

（ii） 每一个代数簇$A\subseteq K^n$，一定存在K^n中无限多个点不属于A。

（iii） 当$n\geqslant 2$时，K^n中每一个超曲面一定含有无限多个点。

3. 设$V(f)$是K^n中一个超曲面，而

$$f=cf_1^{k_1}\cdots f_s^{k_s}\in K[X]$$

是f被分成$K[X]$中不可约多项式的幂的一个分解，其中$f_1,\cdots,f_s$是$K[X]$的不可约多项式，并且两两不相伴，$0\neq c\in K$，$k_i>0\,(1\leqslant i\leqslant s)$。证明$I(V(f))$由乘积$f_1\cdots f_s$生成。

4. 证明，K上两个不定元的多项式环$K[X_1,X_2]$中，素理想只有以下三种类型：

（i）(0)；(ii)由一个不可约多项式f所生成的主理想(f)；(iii)极大理想(X_1-a_1,X_2-a_2)，这里$a_1,a_2\in K$。

5. 设$\sum\limits_{i=1}^{n}a_{ij}x_j=b_i\,(1\leqslant i\leqslant m)$是$K$上一个线性方程组，$A$和$\bar{A}$分别是它的系数矩阵和增广矩阵。令$f_i=\sum\limits_{i=1}^{n}a_{ij}x_j-b_i$

$\in K[X]$ $(1 \leqslant i \leqslant m)$。证明以下两个条件等价：

（i） 秩 $A <$ 秩 $\bar{A}$；

（ii） 存在 $c_1, \cdots, c_m \in K$，使得 $\sum_{i=1}^{m} c_i f_i = 1$。

6. 证明以下两个条件等价：

（i） 对于 $K[X]$ 中每一个理想 $\mathfrak{a} \neq K[X]$ 来说，都有 $V(A) \neq \varnothing$（Hilbert零点定理）；

（ii） 设 B 是 K 上有限生成的交换环。如果 B 是域，则 B 是 K 上有限次（代数）扩域（定理 5.2.9）。

附　　录

I．Zorn 引理

设A是一个非空集．在A上定义了一个关系，用符号$\leqslant$表示．如果下列条件被满足，就称A（对于这个关系来说）是一个**偏序集**：

1°　自反性：对于任意$a\in A$都有$a\leqslant a$；

2°　传递性：如果$a\leqslant b, b\leqslant c$，则$a\leqslant c$；

3°　反对称性：如果$a\leqslant b, b\leqslant a$，则$a=b$．

例如，设M是一个非空集，A是M的一些子集所组成的集．则A对于集的包含关系"$\subseteq$"来说作成一个偏序集．

以下设A是一个偏序集．

A的一个元素a叫做A的一个**极大元素**，如果对于任意$b\in A$来说，只要$a\leqslant b$，就必然有$a=b$．

设B是A的一个非空子集．$a\in A$叫做B的一个**上界**，如果对于任意$b\in B$来说，都有$b\leqslant a$．

A的一个子集C叫做一个**链**，如果对于任意$a, b\in C$来说，或者$a\leqslant b$，或者$b\leqslant a$．

Zorn引理　设A是一个偏序集．如果A的每一个链都有一个上界，则A含有一个极大元素．

设A是一个偏序集．如果A的每一个链都有上界，那么就称A是一个**归纳集**．Zorn 引理是说，每一个归纳集都含有一个极大元素．

Ⅰ. 基数

设A，B是两个集．如果存在一个双射，$A\to B$，那么就说A与B是**对等的**，并且记作$A\sim B$．

集的对等显然具有自反性，对称性和传递性．彼此对等的集组成的类叫做集的**对等类**．每一个集属于且只属于一个对等类．

一个集A所在的对等类叫做A的**基数**．A的基数用符号$|A|$来表示．

根据这个定义，每一个集有唯一的基数；两个集A与B有相同的基数必要且只要$A\sim B$．

令$I_0=\varnothing$．设n是一个正整数．令$I_n=\{1,2,\cdots,n\}$是前n个正整数所组成的集．容易证明，$I_m\sim I_n$当且仅当$m=n$．因此，我们把I_n的基数$|I_n|$与n等同看待．

一个集A如果与I_n对等，就说A含有n个元素．与某个I_n（$n\geqslant 0$）对等的集叫做**有限集**，否则叫做**无限集**．根据以上的理解，一个有限集A的基数$|A|$就是A所含元素的个数．

自然数集$Z=\{1,2,3\cdots\}$的基数记作$\aleph_0$（读作aleph零）．基数为$\aleph_0$的集（即与自然基集对等的集）叫做**可数集**．整数集Z，有理数集Q都是可数集，而实数集R则不是可数集．

设α,β是两个基数．A,B是两个不相交的集，$|A|=\alpha$，$|B|=\beta$．α与β的和$\alpha+\beta$定义为并集$A\cup B$基数$|A\cup B|$；α与β乘积$\alpha\beta$定义为集合积$A\times B$的基数$|A\times B|$．

设α,β是两个基数．A,B是两个集，分别以α，β为基数：$|A|=\alpha$，$|B|=\beta$．α说是**小于或等于**β，记作$\alpha\leqslant\beta$（或$\beta\geqslant\alpha$），如果A与B的一个子集对等．α说是（**严格**）**小于**B，记作$\alpha<\beta$（或$\beta>\alpha$）．如果$\alpha\leqslant\beta$且$\alpha\neq\beta$．

容易验证，基数的加法和乘法以及大小的定义是没有歧义的，即不依赖于集A和B的选取．

下面是关于基数的一些基本事实。这些事实的证明都不太困难。然而我们只把它们罗列在下面而略去证明。读者可以参看有关集论的书籍(例如，Hausdorff，集论(中译本)，科学出版社，1960)。

1° 设 A，B 是两个集。如果 $|A|\leqslant|B|$ 且 $|B|\leqslant|A|$，则 $|A|=|B|$。

2° 对于任意两个基数 α 与 β 来说。

$$\alpha<\beta,\ \alpha=\beta,\ \beta<\alpha$$

三种情形必有一种且仅有一种成立。

对于基数 α,β,γ 来说，

$$\alpha\leqslant\beta,\ \beta\leqslant\gamma\Longrightarrow\alpha\leqslant\gamma.$$

3° 任意一个无限集都含有一个可数子集。因此，对于任意一个无限基数 α 来说，都有 $\aleph_0\leqslant\alpha$。

4° 设 α 是一个无限基数，β 是一个基数，且 $\beta\leqslant\alpha$。则

(i) $\alpha+\beta=\alpha$； (ii) $\alpha\beta=\alpha$。

特别，我们有

5° $\alpha+\aleph_0=\alpha,\ \alpha\aleph_0=\alpha$，若 α 无限；

$\alpha+\aleph_0=\aleph_0,\ \alpha\aleph_0=\aleph_0$，若 α 有限。

6° 令 A 是一个集，n 是一个正整数。$A^n=\overbrace{A\times\cdots\times A}^{n}$。

(i) 如果 A 是有限集，则 $|A^n|=|A|^n$；

如果 A 是无限集，则 $|A^n|=|A|$。

(ii) $\left|\bigcup_{n\in N}A^n\right|=\aleph_0|A|$。

7° 设 A 是一个无限集。令 $F(A)$ 表示 A 的一切有限子集所组成的集。则 $|F(A)|=|A|$。

名词索引

七 画

八 画

九 画

十 画

十一 画

十二 画

十四 画

十六 画

其 它

[General Information]
书名=域论基础
作者=郝鈵新
页数=233
SS号=10100840
出版日期=1988年02月第1版

前言
目录